Approved by

Cosmin Ghita,

General Manager,

Endorsed by

Mihai Sandulescu,

DAMR Director

INFORMATIVE NOTE
to the shareholders related to the implementation of the Regulation 2016/679 (GDPR – General Data Protection Regulation) within SN Nuclearelectrica SA

1. Context

The Regulation 2016/679[1] has been issued in order to achieve a better protection of the fundamental rights and freedoms of natural persons (namely the protection of natural persons with regard to the processing of personal data), as well as in order to standardize this protection and the legislative framework at the EU level and with regards to the EU citizens from this perspective, even if the data controllers are based outside the European Union.

Given the complexity of the compliance with the Regulation and the significant costs for the controllers who process personal data (e.g. insurance, banks, data services, medical services) a period of two years has been established (from the issuance of the Regulation on 27.04.2016 until 25.05.2018) in which the organizations to which the Regulation applies must take all the technical and organizational measures for compliance.

The Regulation has entered into force automatically (without transposition to the national legislation / law).

2. The impact of the Regulation 2016/679 (executive summary)

The Regulation 2016/679 replaces the prior legislative framework (Law 677/21.11.2001[1] for the

[1] (EU) Regulation 2016/679 of the European Parliament and of the Council of 27.04.2016 on the protection of natural persons regarding the processing of personal data and the free movement of such data and on repealing the Directive 95/46/EC (General Data Protection Regulation).
[2] Repealed by Law no. 129/15.06.2018 for amending and supplementing the Law no 102/2005 on the establishment, organization and functioning of the National Supervisory Authority for Personal Data Processing, as well as for repealing the Law no. 677/2001 for protection of persons with regard to the processing of personal data and the free movement of such data

protection of persons with regard to the processing of personal data and the free movement of such data and the Directive 95/46/EC), bringing some changes related to:

a) **material applicability**: The Regulation applies to all the personal data processing operations (extension of the definition of personal data and inclusion of new definitions):
   - processing: any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
   - 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 several factors specific to his/her physical, physiological, genetic, mental, economic, cultural or social identity; examples: name/first name, Personal Identification Number, series/number of the identity card/identity document/passport, medical data, photo, home/residence address, digital fingerprints/papillary traces, voiceprint, iris scan, biometric data, DNA, blood vessel prints (if any), URL of personal blogs, personal webpages, personal QR code, audio/video recordings (including internal video and perimeter surveillance), access recordings, income (pay slips, bank statements), kinship relationships, e-mail address, IP address, information about the internet traffic (addresses accessed, websites viewed, clicks), phone number, signature, age, date of birth, position, work history and assessment, test results (e.g. medical, driving), data about the properties which may identify a person (e.g. vehicle registration number, chassis series, housing cadastral number), GPS coordinates

b) **territorial applicability**: The Regulation applies:
   - to the processing performed by a controller or a processor based in the EU,
   - to the processing of personal data of persons in the EU carried out by a controller or a processor who is not based in the EU (significant extension of the geographical scope of the European Union regulations in the field of personal data), if goods and services are provided to persons located in the EU (even if a payment is not involved), the behavior of the persons in the EU is monitored,

c) the controllers must implement appropriate **technical** (e.g. IT and physical security) **and organizational measures** (procedures, codes of conduct, interdictions, authorizations, verifications, permissions) to meet the requirements of the Regulation and to protect the rights of the data subjects,

d) in order to know what (categories of) personal data they hold and for what purpose, the organizations to which the Regulation applies must undertake **a mapping of personal data** and of the processing performed on them (data mapping – record of the processing activities / art 30) by which they should identify at least:
   - the categories of data subjects,
   - the categories of personal data,
   - the purposes of the processing,
   - the categories of recipients,
   - the cross-border transfers of data,
   - the deadlines for the erasure of the different categories of data,
   - the technical and organizational security measures,

e) an **impact analysis** (DPIA – Data Protection Impact Analysis) must be made for the processing likely to generate high risk, an analysis which implies:
   - prior consultation of the supervisory authority,
   - description of the data processing,
   - analysis of the data processing principles,
   - identification and analysis of risks (including the estimation of the occurrence likelihood and of the potential impact) and of the potential risk sources,
   - implementation of the risk removal/reduction measures,
   - consultation with the DPO, the data subjects

f) higher standards for obtaining the **consent**:
   - freely expressed: unconditioned by the provision of the service, the lack of the subordination relationship,
   - specific and granular: expressed for each type of processing and processing purpose,
   - informed: existence of an appropriate and documented information,
   - unequivocal: clear identification of the subject matter of the consent,
   - clear and positive action: the silence or abstention does not represent a consent,
   - documented: existence of a record of the consent expressed on hardcopy or in electronic format,
   - the withdrawal of the consent must be made as easily as its granting,

g) increased **transparency**: the need to inform the data subjects (e.g. employees, shareholders, contractors) about the rights they enjoy, which involves the development of procedures and processes of information and communication with the data subjects, information forms and an information of the staff, shareholders and partners,

h) recognition of **new rights** of the data subjects: information, access, rectification, erasure, restriction, portability, objection, automated decisions and profiling, restrictions,

i) the need to appoint a **data protection officer** (DPO), under certain conditions of independence and lack of a conflict of interest with other professional tasks, with the need to allocate resources for his/her work (time, equipment, training, budget and access to personal data and related processing operations), and having specific roles:
   - actual involvement in all the aspects related to data protection, including regular participation in the meetings of middle/senior management and support/ involvement in case of occurrence of a security incident,
   - advise of the management on the specific obligations and vulnerabilities identified,
   - facilitation / coordination of the plans for implementing the Regulation
   - training of the management and employees on their obligations,
   - facilitation of the preparation of the documentation / procedures for data mapping, data protection impact assessment (DPIA), internal procedures for applying the Regulation,
   - point of contact for the data subjects and the supervisory authority,
   - monitoring of the organization's activity to facilitate compliance,

j) the obligation to immediately notify to the supervisory authority the cases of personal **data breach** and, in the situation of high risks related to the personal data, the data subject as well
   - the data breach: the data breach leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

k) The Regulation requires the controllers to demonstrate/maintain a documented record regarding the way of complying with the requirements of the Regulation, namely **to**

document the compliance and the way of obtaining the internal assurance related to compliance, which represents a significant change in the exercise of authority by the supervisory authority,

l) The revision and modification of the internal regulatory framework (procedures, processes) which addresses data and personal data processing,

m) **corrective competences** of the supervisory authority: the Regulation offers indications of the degree of application of the corrective competences of the controllers who do not comply with the provisions of the Regulation (the Regulation lists the competences from the least severe to the most severe), but it does not provide the security of their application in the order in which they are mentioned in the Regulation. Corrective competences: warnings, reprimands, orders, obligations, temporary or definitive limitations on processing, withdrawal of certifications, imposition of administrative fines (up to EUR 20 million or 4% of the global turnover), suspension of cross-border data flows.

3. Measures implemented by SN Nuclearelectrica SA

In order to comply with the Regulation, SNN SA has implemented a set of technical and organizational measures and has undertaken actions for compliance and/or implementation of the requirements of the Regulation as follows:

a) a working group which makes the analysis of the impact of the new regulations on the company's organization and functioning and the plan including the measures which must be implemented has been appointed,

b) the first impact analysis of the provisions of the Regulation has been made, which generated a preliminary identification, for each provision, of the applicability with regards to SNN, the legal basis, the context and additional explanations for its understanding and/or application, as well as actions proposed and persons responsible for their implementation; a similar analysis related to the human resources aspects has been made in CNE Cernavoda,

c) the areas and the lines of action (indicative / preliminary action plan) for implementing the requirements of the Regulation have been identified,

d) a data protection officer has been appointed (and notified to the supervisory authority), having the responsibility to inform and advise the SNN management and staff with regards to their obligations in the field of data protection and implementation of the Regulation,

e) the data protection officer has conducted awareness and training sessions for the inventory of the personal data processing (data mapping) with the departments in the Headquarters and in the subsidiaries,

f) a record of the personal data processing activities has been made (data mapping, according to art 30 of the Regulation), with the participation of all the organizational structures within SNN,

g) a set of internal procedures which address the essential aspects of the Regulation has been issued:
    a. General procedure for personal data protection within SNN SA,
    b. Procedure for response in case of personal data breach,
    c. Processing of personal data of the SNN staff,
    d. IT policy for personal data processing within SNN SA,

h) The SNN website has been modified, being updated with:
    a. The policy for personal data processing and protection within SNN,
    b. Information of the public about the personal data processing within SNN SA, its

rights and the manner of exercising such rights,

c. Information of the candidates in the vacancies contest about the personal data processing during the selection process, the candidates's rights and the ways of exercising these rights,
d. Contact details of the data protection officer

i) the standard contractual clauses for updating the commercial contracts in which SSN is a party have been established and the process for signing the necessary addenda has been initiated,

j) the information forms for the employees, contractual partners, shareholders, public and media have been prepared,

k) the consent forms for the employees and commercial partners have been prepared,

4. Future actions

Following the meetings held in the period of implementation of the essential package of measures, a list of actions which must be further implemented has been identified, and these (or their amended versions following the internal analyses) will be gradually implemented in the next period.

Among these we can mention:

a) Apointment of a working group which coordinates and supports, through an integrated and unitary coordination (CNE Cernavoda- Executive SNN -FCN) the correct and complete implementation of the requirements of the GDPR Regulation, with the issuance by the General Manager of a decision in this respect,

b) Extension/ detailing of the analysis made within the data mapping exercise (record of personal data and of the processing performed on them) in order to check the completeness of consideration of all the departments / divisions of CNE Cernavoda which process personal data and establishment of procedures at the level of the departments, by means of IDP, for the personal data processing activity,

c) Identification, following the extension/detailing of the analysis made during the data mapping exercise, of the additional measures which must be implemented if applicable,

d) Gradual revision of the internal regulatory framework in order to update the internal regulations for compliance with the requirements of the Regulation,

e) Development of an internal programme for communication, training and awareness of the SNN staff related to the requirements of the Regulation,

f) Independent assessment of the degree of compliance with the requirements of the GDPR Regulations in all the SNN units (it is advisable to be made by a competent external company) after the implementation with internal resources.

…….
Ovidiu Bordeut
Data Protection Officer
Risk Management Department, Executive SNN