This "ANNEX VIII ROMANIA" is implemented to the procurement agreements for supply, services and works regulated by Romanian law in force and concluded between a company member of ENEL Group and a Contractor.

CONTENTS

1. SCOPE OF APPLICATION.

1.1. This Annex Romania shall apply to all agreements for works/services/supply regulated by Romanian legislation, concluded between a company of ENEL Group and the Contractor.

1.2. This document is part of the General Conditions.

1.3. Notwithstanding the provisions of art."Scope" of the General Part, the Agreement includes the webpage where the General Part and this Annex Romania are available; under any circumstances, a copy shall be submitted to the Contractor.

1.4. Understanding the provisions of art. "INTERPRETATION AND HIERARCHY" of the General Part, any waiver or modification of this Annex Romania proposed by the Contractor shall be valid only if it is made in writing and accepted in the same form by ENEL and it shall be applied only to the Agreement which it was proposed for, excluding the possibility that the exception can be extended to other agreements in progress or which shall be eventually provided later by the same Contractor.

1.5. It is specified that if any discrepancy or inconsistency between the documents that are part of the Procurement Agreement occurs, reference shall be made to art. "INTERPRETATION AND HIERARCHY"" of the General Part, which specify that the prevalence is determined by sequentially order according to which the contractual documents are listed.

1.6. In case that a part of the clauses contained in the General Part shall be amended by agreement of the parties, this amendment shall be indicated in the Agreement/FA by way of derogation from Annex Romania.

1.7. The original version of this Annex Romania is in Romanian language. Please take into account that in case of discrepancy between the original version in Romanian language and translations into other languages, the original version in Romanian language shall prevail.

2. DEFINITIONS.

In addition to paragraph of the General Part in this Annex Romania the following definitions shall be applicable. In this document the following terms shall construed as follows:

a) **ENEL:** any company of ENEL Group Romania;

b) **Agreement:** written agreement concluded between ENEL and the Contractor for the performance of a works services or products Agreement;

c) **Framework Agreement (FA):** written agreement concluded between ENEL and one or several Contractors, aimed to establish the essential elements/ conditions that shall regulate the Procurement Agreements to be awarded in a given period, in particular regarding the price and, where appropriate, the quantities taken into account;

d) **Subsequent contract:** the agreement is the act of will of the two parties concluded, based on an FA between "ENEL" as the "Beneficiary/Purchaser", and one or several business operators as "Contractor";

e) **ENEL and Contractor:** the Contracting Parties, as they are listed in this document;

f) **Price of the Agreement/FA:** the price payable by ENEL to the Contractor, based on the Agreement/FA for the full and proper performance of all its obligations taken by this Agreement;

g) **Day:** calendar day;

h) **Year**: 365 days;

i) **Annex Romania**: this document, an integral and substantial part of the **General Conditions** applicable to ENEL Group, of which this is an Annex, which is supplemented by the Special conditions specific for each type of contract to be concluded by ENEL with a Contractor

j) **Object of the Agreement/FA**: the object of the Agreement/FA is that determined by the Agreement/FA and by the documents that are an integral part of it.

3. APPLICABILITY.

The Agreement/FA shall enter into force on the date when it is signed by both parties.

4. LANGUAGE OF THE AGREEMENT.

Notwithstanding the provisions of art. "LANGUAGE OF THE AGREEMENT" and of art. "INTERPRETATION AND HIERARCHY" of the General Part, the original version of all contractual documents, including the General Part, will be Romanian language. The Agreement/FA and any other document related to the Agreement/FA are concluded in Romanian language, as a compulsory condition.

5. COMMUNICATIONS.

5.1. In addition to the provisions of art. "COMMUNICATIONS" of the General Part, any communication between the parties in connection with the execution of the Agreement/FA, must be done in writing - by letter, electronic means, by written confirmation of receipt of the communication.

5.2 Any written document must be registered both when sent and when received.

5.3 When the contractual documents refer to statements, - notifications, documents for which the signature is required, are admitted only on hard support (on paper).

5.4 Communications must be sent to the addresses (including e-mail address) specified in the Agreement/FA.

5.5 Any Contracting Party can change its contact information by submitting a communication to the other Party with a notification of five (5) business days.

5.6 The Contractor must observe and immediately execute any communication received from ENEL, without any further formality, even in cases when it intends to express its own comments.

6. CONTRACTING CLAUSES CONCERNING THE PRICE.

6.1 In addition with art. "PRICE" of the General Part, for activities provided, payments due by ENEL to the Contractor are those stated in the financial proposal, attached to the Agreement/FA. Prices remain fixed during the period of the Agreement/FA unless the Agreement/FA specifies otherwise.

6.2 In addition to the provisions of art. "INVOICING" of the General Part, invoices will have attached the appropriate supporting documents, as the case may be. In the case of services, the invoices will be supported by supporting documents (e.g. activity annexes, reports, minutes, correspondence, etc.), that will attest to the effective performance of those services.

6.3 Update the contractual PRICE/FAP (Regulation of Price).In compliance with the provisions art. "PRICE" of the General Part, the contracting prices can be adjusted only if this possibility is provided in the Agreement/FA and/or required by applicable law.

6.4 The adjusted prices are applicable exclusively to the activities ordered by ENEL following the date of revision. The price adjustment is requested by the party interested and calculated in line with the modalities indicated in the Agreement/FA; if it is calculated by the Contract, ENEL reserves the right to perform a verification.

6.5 Remuneration of price adjustment. The application of the price adjustment referred to in this section represents for the both parties the full recognition of all the related rights resulting from the changes of costs, which can consist in their increasing or decreasing.

6.6 The value of price adjustment does not contribute to the establishment or achievement of the Contract value.

6.7 Notwithstanding the provisions of art. “INVOICING” of the General Part, invoicing will be done in accordance with art. "Outside electronic systems.", unless stated otherwise by contract.

7. TAXES.

In addition to the provisions of art. "TAXES" of the General Part, the tax residence certificate as stipulated in the General Part will be provided by the Contractor every year along with the first invoice issued in that year, in order to be applied the provisions of the convention for the avoidance of double taxation in force between the two countries. Otherwise, ENEL will be able to make deductions in compliance with applicable legal provisions.

8. AMENDMENT OF THE AGREEMENT.

In addition to the provisions of art. “CHANGES TO CONTRACTUAL TERMS” of the General Part, the Contracting Parties have the right, during the Agreement/FA, to agree on amendment of the provisions of the Agreement/FA, by written addendum concluded in compliance with applicable legal provisions.

9. SUBCONTRACTING.

9.1 In addition to the provisions of art. “ASSIGNMENT OF THE CONTRACT AND SUBCONTRACTING” of the General Part, the Contractor can use subcontractors after the Contract is signed by both Parties, therefore during the performance of the agreement, only with the ENEL’s approval.

9.2 The Contractor has the obligation to submit at the conclusion of the Agreement/FA, all the agreements concluded with subcontractors appointed which must indicate in detail all the activities they shall provide and the value threshold for each type of activity.

9.3 The List of Subcontractors, including their identification data and agreements concluded with them, are considered annexes to the Agreement/FA.

9.4 The Contractor can change any subcontractor only if it has not fulfilled its part of the Agreement/FA. Changing a Subcontractor shall not alter the price of the Agreement/FA and it shall be effective only if the approval of ENEL was obtained in advance.

9.5 If during the performance of the Agreement/FA, the Contractor requires employment of subcontractors to fulfil the Agreement/FA, it will not have the permission to do so without prior consent of ENEL and only up to a limit of 30% of the main activity, in case of works performance agreements and 30% of the contract value for service agreements and 30% of the value of installation/fitting services for supply contracts. In case it obtains this consent, the Contractor shall submit to ENEL, the certified copy of the contract concluded with the subcontractor mentioned, which, thus, becomes an annex to the Agreement/FA.

9.6 According to the provisions of art. “CONTRACT ASSIGNMENT AND SUBCONTRACTING” of the General Part, the Contractor who will execute a contract, can use a self-employed worker to perform a certain part of that contract. The self-employed worker has the same rights and obligations as a Subcontractor, but is not included in the percentage of subcontracting (30%).

9.7 The Contractor is not allowed, under any circumstances, to subcontract parts of the works under the scope of the agreement awarded to it, if it did not receive written consent of ENEL. In case that, following the inspections carried out by authorized personnel of ENEL, it is found out that the Contractor has provided works with subcontractors previously authorized by ENEL or Subcontractors of the Subcontractors, ENEL reserves the right to terminate the agreement and to claim damages.

9.8 The Contractor has the obligation to conclude agreements with the subcontractors appointed under the same terms according to which it signed the agreement with ENEL.

9.9 The Contractor has the obligation to inform the Subcontractors regarding all the documents part of the agreement between the Contractor and ENEL that have an influence on the execution of the agreement.

9.10 The Contractor is fully responsible to ENEL on the modality the subcontractors fulfil their part of the Agreement/FA.

9.11 The Contractor has the obligation to submit to ENEL the proof of payment regarding the invoices issued by the Subcontractor in connection to the performance of the Agreement/FA. Also, the direct payment to the Subcontractor is permitted in the conditions prescribed by art. 232 paragraph (2)-(3) of Law no. 99/2016.

10. CESSION.

10.1 Notwithstanding the provisions of art. “ASSIGNMENT OF RIGHTS AND RECEIVABLES” of the General Part, during the execution of the Agreement/FA, only the assignment of claims arising from the Agreement/FA is permitted, the obligations undertaken still remaining the liability of the Contracting Parties, as they have been initially provided and assumed.

10.2 The assignment of debt shall not relieve the Contractor of any responsibility regarding the guarantee or any other obligation taken by the Agreement/FA.

10.3 Nevertheless, the cession of the contract is possible only in the cases expressly stipulated in art. 240 of Law no. 99/2016, provided that the conditions within art. 235-243 are met.

11. PROVISIONS CONCERNING THE EARLY CESSATION/TERMINATION OF THE AGREEMENT/FA.

Notwithstanding the provisions of art. "Termination for reasons attributable to the Contractor" of the General Part, termination can be decided only under the conditions provided in the Particular Conditions specific to each type of contract, an integral part thereof.

12. EARLY TERMINATION OF THE AGREEMENT ON OCCURRENCE OF CERTAIN UNFORESEEN CIRCUMSTANCES.

12.1 In addition to the provisions of art. “Withdrawal” of the General Part, ENEL reserves the right to terminate for convenience the Agreement/FA, without any compensation to the Contractor, by written notification to the Contractor within 30 days following the occurrence of circumstances which could not be foreseen at the conclusion of the Agreement/FA and which lead to amendment of the contracting terms to the extent that performance of the respective agreement would be contrary to its business interests. The termination for convenience of the Agreement/FA shall be effective from the date specified by ENEL in the content of the notification.

12.2 In this case, the Contractor has the right to claim only the payment for the part of the Agreement/FA fulfilled until the termination for convenience of the Agreement/FA.

13. ORDINARY EARLY TERMINATION OF THE AGREEMENT.

13.1 In addition to the provisions of art. “Withdrawal” of the General Part, ENEL can terminate the Agreement/FA at any time and at any stage of the contract.

13.2 The termination shall be notified to the Contractor by a written notification with receipt acknowledgement and it shall produce effects upon receipt by the Contractor.

13.3 In case that ENEL claims the termination of the Agreement/FA, the Contractor is entitled to claim damages, compensations of up to 10% (ten percent) of the contract value undelivered (i.e. of the minimum value undelivered of the FA).

13.4 Notwithstanding the provisions of art. “SUSPENSION” of the General Part, with the payment of the remuneration referred to in the preceding paragraph, the Contractor cannot raise other claims, regardless of their nature.

14. TERMINATION IN SPECIAL CASES OF INSOLVENCY.

The Agreement/FA can be also terminated in advance, in case that the procedure of dissolution, reorganization or insolvency proceedings have been initiated on one of the parties, provided that it must be done in compliance with the procedures and provisions of the applicable law.

15. GOOD PERFORMANCE BOND.

15.1 In addition to the provisions of art.“ECONOMICl GUARANTEE” of the General Part, the amount of the Good Performance Bond of the Agreement is 10% of the contract value, excluding VAT.

15.2 The Good Performance Bond shall be established as follows:

By an instrument of guarantee issued under the conditions of the law by a bank or an insurance company and it shall be considered as an annex of the agreement. The guarantee instrument shall be submitted in original at the headquarters of ENEL and it shall include the following, as a compulsory condition:

- the Contracting Parties (Insurer/Bank - the issuer of the policy, Insured-Contractor, Beneficiary-ENEL
- the obligation of the bank or of the insurance company to pay in favour of ENEL, any amount up to the limit of the Good Performance Bond, unconditionally/conditioned, accompanied by a statement regarding the failure of the Contractor to fulfil its obligations, any eventual payments to be made within the term specified in the request, with no further formalities from ENEL or the Contractor;
- the period of validity of the Good Performance Bond.

15.3. Good Performance Bonds shall be returned upon request, in writing, to the Contractor as follows:

(1) In case of supply contract, ENEL has the obligation to issue/return the Good Performance Bond within no more than 14 days following the date of the products acceptance report covered by the agreement and/or following payment of the final invoice, if, until that date, any claims were not raised concerning it.

(2) In case of service contract, ENEL has the obligation to issue/return the Good Performance Bond within no more than following the date of completion by the Contractor of its obligations taken by this agreement, if, until that date, any claims were not raised concerning it.

(3) In case of Design Contracts, ENEL has the obligation to issue/return the Good Performance Bond as follows:

a) the value of the Good Performance Bond related to pre-feasibility and/or feasibility surveys within 14 days following the date of delivery and receipt/approval of the respective technical and economic documentation, if, until that date, any claims were not raised concerning it;

b) the value of the Good Performance Bond related to the technical documentation and/or performance details, within 14 days following the conclusion of the report at the completion of works executed in accordance with the related project, if, until that date, any claims were not raised concerning it.

(4) In case of works contracts, ENEL has the obligation to issue/return the Good Performance Bond as follows:

a) 70% of the Good Performance Bond value, following the conclusion of the report at the completion of works executed and commissioning of such works, if the acceptance is performed without any reserves and the risk for latent defects is minimum;

b) the remaining of 30% of the Good Performance Bond value, at the expiry date of the works performed, based on the final acceptance report.

15.4 In case the Contractor chooses to establish the Good Performance Bond by a letter of guarantee, it shall be able to choose the following methods to establish the guarantee to indicate the two distinct periods mentioned above in par. (4) a) and b).

15.5 It shall either request the issuing bank the issuance of two letters of guarantee with different validity periods, but which together can cover the value and validity indicated above or it shall request a single letter of guarantee for the entire period of validity, and at the first instalment reimbursement, it shall request the bank to amendment thereto for the period and the amount remaining. ENEL shall not deliver the original letter until the expiry of 24 months guarantee period for the works performed, thus the additions of the letter shall be requested to the bank without submitting of the original thereof.

15.6 ENEL has the right to raise claims on the Good Performance Bond, within the limit of the damage caused if the Contractor fails to fulfil its obligations taken in accordance to this contract. Prior to issuing a claim on the Good Performance Bond, ENEL has the obligation to communicate this to the Contractor, specifying the obligations which have not been observed.

16. INSURANCE.

Art. "INSURANCE" of the General Part will be completed by the conditions set out in the Particular Conditions specific to each type of contract, part of contract, or in the FA/Contract.

17. PERSONAL DATA PROTECTION.

17.1 Notification concerning the personal data processing provided for the purposes of this contract

17.1.1. For the purposes of this Contract as regards definitions concerning personal data, express reference must be made to EU Regulation 2016/679 (hereafter GDPR) and any other current legislation in force, including Romanian Law no. 190/2018 related to GDPR's implementation.

17.1.2 Without prejudice to the terms set forth above, the parties are informed that the personal data are acquired reciprocally during the tender procedure for assigning the Contract, and processed for purposes closely linked with the management and execution of the Contract, or to enable the execution of the duties envisaged by the law. Additionally, personal data will be collected and processed using both automated means and in paper form and will be stored for the entire duration of the Contract and after its termination for a period not exceeding the terms envisaged by applicable laws.

In this respect and taking into consideration the capacity of the provider/supplier as data processor, respectively the capacity of the client/beneficiary as data controller within the meaning of the provisions of GDPR, it should be noted that:

- the Data Controller for the data in question is the Client Company of the ENEL Group[1], in the person of its legal representative *pro tempore* (hereinafter "ENEL");
- The data subject is the natural person whose personal data are processed for the purposes of concluding, management and execution of the Contract (hereafter the data subject);
- The personal data processed may be transmitted to third parties, *i.e.* to companies subject to management and coordination by ENEL S.p.A. or connected with the Data Controller, or to other subjects. The above-mentioned third parties might be appointed as Data Processor, when requested by GDPR provisions;
- The data subject is entitled to exercise the rights envisaged in Articles 15-21 of the GDPR (right to access data, request their rectification, portability or cancellation, request the limitation of processing of data concerning him/her or may oppose processing), where applicable, by contacting the Data Controller;
- The data subject is entitled to lodge a complaint to the Romania Data Protection Authority (ANSPDCP), with registered office in Bucuresti, B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, cod postal 010336, Romania, Tel. (+40) 318059211 or (+40) 318059212 , email: anspdcp@dataprotection.ro;
- The Data Controller has appointed the Data Protection Officer (DPO) pursuant to Article 37 of the GDPR, whose contact details can be found on the Data Controller's website.

17.1.3. This Annex shall be mandatorily supplemented and interpreted with all and any provision of the GDPR and/or any national and/or European secondary legal rules regarding the personal data processing operations, both the Processor and the Controller agree that in the case of amending the legal framework and/or any of the applicable legal provisions, the validity, lawfulness and enforceability of the remaining provisions hereof shall not be affected or damaged in any way. To this end, both parties undertake to make reasonable efforts to introduce/amend/replace the provision become invalid/unenfoceable.

17.1.4. The contract management form a data protection perspective shall be also the responsibility of the contract managers nominated by each Party (for instance, but not limited to: transmission of the data breach notices, change of the sub-processors/authorized personnel etc.) in accordance with the Contract.

17. 2 Appointment of the Supplier as Personal Data Processor

17.2.1. On signing the Contract and for its entire duration, the Data Controller, appoints the Supplier, who accepts, as Personal Data Processor, pursuant to and for the purposes of Article 28 of the GDPR .
If the Supplier is a Temporary Consortium of Companies (RTI)/Ordinary Consortium or a Stable Consortium, the companies belonging to the Temporary/Ordinary or Stable Consortium and the executing companies are appointed as data processing managers.

17.2.2. The Supplier undertakes to carry out personal data processing operations in compliance with the duties imposed by the GDPR and the instructions thereafter issued by the Data Controller.
It is agreed that if the Supplier defaults on the duties as per this document, the Data Controller has the right to terminate the Contract, by a written notification and to claim damages, without no other formality, under Article 1553 of the Romanian Civil Code and the Supplier represents that it acceptes expreselly and without no reservation the provision of this clause. Termination becomes effective on the date communicated within the notice.

17.2.3 Duties and instructions

17.2.3.1 Whereas the Supplier, in relation to its declared experience, capacity and reliability, has provided a suitable guarantee of full compliance with the applicable data processing regulations and the GDPR, its duties and responsibilities are defined, by way of example and without limiting to the above, as follows:

a) They must only process personal data when instructed to do so by ENEL, registered in a document in which the type of data processed and the categories of Data Subjects are listed (Annex GDPR 1);
b) They will have to appoint Authorized Persons for processing personal data ("Authorized Persons") to carry out of any operation, including simple consultation, concerning processing personal data entered in IT systems/applications/infrastructure or paper files held by ENEL, using the specific template provided by ENEL (Annex GDPR 2); Before starting the activities covered by this Contract or otherwise by the date specifically communicated by ENEL, the Supplier will also send ENEL its own declaration concerning the appointment and list of names of its employees/collaborators as "Authorized Persons" for data processing using the template provided by ENEL (Annex GDPR 3);
c) They must ensure that the nominated Authorized Persons for processing personal data have undertaken to observe both the legal dispositions stipulate within GDPR and/or within the applicable national laws, as well as Data Controller's instructions and also maintain the confidentiality both of the information and personal data coming to their knowledge as a consequence or even only during the execution of the Contract and not to communicate them to other third parties, unless expressly authorised to do so by the Data Controller and except for the cases expressly

[1] Company of the ENEL group that establishes the Contract or the company in the name and on behalf of which this is established

envisaged by law; the Data Controller reserves the right to request the Supplier to provide the list of Authorized Persons for data processing in order to comply with obligations under the GDPR or other legal requirements or for reasons of national security or public interest;

d) They must adopt all the security measures as set forth in Article 32 of the GDPR, as well as all other preventative measures dictated by the experience and/or by the international/European best practices designed to prevent any processing of the personal data that is not allowed or not compliant with the purposes for which the personal data are processed; they must also ensure that they collaborate effectively in implementing these measures, in notifying and communicating any breaches of the personal data and in assessing the impact on the data protection, if requested by the Data Controller, in order to ensure the confidentiality and security of the data and minimise the risks that the data in question might be accidentally destroyed or lost;

e) On express request ofENEL, they will have to provide the list of countries and data centres where personal data are processed on behalf of ENEL;

f) hey may transfer the data to a third country or to an international organisation located outside the European Union only in cases envisaged and under the conditions defined by the GDPR, unless this is required by the law of the European Union or the national law to which the Supplier is subject. In this case, the Supplier undertakes to inform promptly ENEL about this legal obligation unless forbidden from doing so for relevant reasons of national security or public interest;

g) Bearing in mind the nature of the processing, the Supplier undertakes to help the Data Controller with its own appropriate technical and organisational measures, to the extent to which this is possible, with a view to fulfilling the duty of the latter to act on the data subject's request to exercise their rights;

h) It must assist the Data Controller in ensuring compliance with the duties set forth in Articles 32 to 36 of the GDPR, in consideration of the nature of the processing and the information available;

i) They must, on ENEL's request, erase and/or return all the personal data once the execution of the services relative to the processing have been completed and erase the existing copies, unless the law of the European Union or its member States envisages that the data be stored, providing the Data Controller with proof that this has been accomplished;

j) When a Data Protection Officer has been appointed pursuant to Article 37 of the GDPR, this must be communicated to ENEL;

k) They must provide the Data Controller with all the information necessary to demonstrate compliance with the requirements of the GDPR by participating in the review activities, including the inspections, carried out by the Data Controller or by another party appointed by the same;

l) In case of actual or suspected personal data breaches, they must promptly notify the Data Controller within 24 hours of becoming aware of the event and without any unjustified delay and in accordance with Annex 9 and has the obligation to document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken;

m) They must cooperate with the Controller by making freely available all necessary information in order to fulfil the obligations defined in Articles 33 and 34 of the GDPR, including current certifications;

n) Over and above the dispositions of Article 30, item 5 of the GDPR, they must keep a register of the processing activities carried out on behalf of the Controller pursuant to Article 30 of the GDPR, which must be exhibited on the request of the Controller, if applicable, in case of events which are regulated by Articles 33 and 34 of the GDPR.

17.2.3.2 It is forbidden to the Contractor to treat the personal data for use different of the scope of contract. Particularly, if it's not needed for the execution of contract, it is forbidden, for example, to the Contractor to massively extract the personal data also using "RPA - Robotic Process Automation" (or "automatic method), unless the committee preventively authorized it.

17.2.3.3. Any and all personal data processing operations shall be exclusively conducted in the European Union Area ("EU".) Any personal processing data operation which involves either the transfer or the access by the natural persons/legal entities outside the EU area shall be strictly forbidden, including when these persons act in the capacity as affiliates of the Processor. Nevertheless, in the case where, for various reasons, it is necessary that the personal data processing operations should be carried on outside the EU area, the processor undertakes to obtain the prior written consent of the Controller. The refusal of the Controller to allow the conduct of the personal data processing operations outside the EU area, may not be deemed as a reason for amendment of the commercial and/or economic/financial conditions assumed by the Parties upon conclusion of the Contract. To this end, the Parties agree that the refusal of the Controller may not be (i) a reason for termination of the Contract due to the fault of the Controller and/or (ii) a reason for increasing the price of the services provided, including as regards the issue of penalties and/or (iii) a reason for non-fulfilment/faulty fulfilment of the contractual obligations assumed by the processor.

17.2.3.4. whenever the processing is based on the consent of the data subjects and only in the case where the Processor is previously authorized, in writing, by Controller to obtain the agreement of the data subjects for the performance of the subject-matter of the Contract, the Processor shall be obliged to prove that the data subject agreed to his personal data processing, as well as to ensure that any consent obtained by the Processor cumulatively meet the following requirements: to be free, to be specific, to be informed, to be unequivocal, to be express and explicit, to be easily distinguished from the remaining communications, to be easily withdrawn ("Conditions pertaining to the consent"). The Processor undertakes to request the consent in a clear and intelligible manner so that the data subjects fully understand the purpose of this request and the effects of granting the consent. Moreover, the Processor is obliged to keep records of the manner of obtaining/withdrawing the consent, avoiding as much as possible to obtain the verbal consent. Moreover, the consent must be obtained for each purpose separately. In the case where, for various reasons, the Processor considers that certain processing purposes are similar, as they may be carried out based on a single consent, the Processor is obliged to inform the Controller, in writing, before the correlation of the purposes pertaining to the processing operations regarding this issue. The Processor is required to keep and send to the Controller, in a structured form, all and any of the records/proofs of the manner of obtaining the consent, respectively of the proofs regarding its existence ("Consent-related proofs"). Last, but not least, in the case where the Processor acts on behalf and in the name of the Controller (for instance, but not limited to: arranges the relationship with the data subjects, gets in touch with the data subjects for the purpose

of submitting offers etc. by virtue of the prior consent obtained by the Controller), the Processor is required to meet all the other Requirements and Proofs pertaining to the consent.

17.2.4 Compensation and Liability

17.2.4.1. Pursuant to Article 82 of the GDPR, the Supplier will be liable damage caused by the processing if it has failed to comply with the duties as imposed by the Contract or has acted in a different or contrary way to Controller's instructions.

17.2.4.2. The Supplier will also be liable in the first person as regards the Controller and interested parties, if an Other Processor appointed by it fails to fulfil his/her duties regarding the protection of personal data.

17.2.4.3. In the event of further damage sustained by the Controller as a result of the conduct of the Supplier or one of its Other Processors, the Controller reserves the right to claim further compensation equal to at least three times the amount of the Contract.

17.2.4.4. The Controller or the Supplier are exonerated from all liability if they can prove that the damaging event is in no way ascribable to them.

17.2.5 Duration

The above-mentioned appointment as Data Processor will be automatically revoked to the Supplier on expiry of the contractual relationship or on its termination for any cause, without prejudice to compliance with all the dispositions of the Article 2.1 above concerning processing still in progress even as regards the fulfilment of contractual requirements.

17.2.6 Other Processor

17.2.6.1. If, for specific processing activities, the Supplier intends to involve in the execution of the Contract subjects outside its own organization, these subjects must be appointed as Other Processors pursuant to Article 28 paragraph 4 of the GDPR (hereafter Other Processors or Other Processor).

17.2.6.2. The Other Processors must comply with the same obligations that this Contract imposes on the data processor (Annex GDPR 4).

17.2.6.3. In particular, in compliance with the dispositions of letters b) and c) of paragraph 2.1 "Duties and instructions", each Other Processor shall in turn appoint any resources used in the processing as "Authorized Persons" for processing personal data, using the appropriate template prepared and including the related instructions (Annex GDPR 7).

17.2.6.4. Before starting the activities covered by the Contract or otherwise by the date specifically communicated by the Controller, the Other Processor will also send the Controller its own declaration concerning the appointment and list of names of its employees/collaborators as "Authorized Persons" for data processing using the template provided by the Controller (Annex GDPR 8);

17.2.6.5. On signing the Contract the Other Processors are thereby authorized (Annex GDPR 5).

17.2.6.6. If the Supplier, for proven and reasonable reasons, intends to entrust services to Other Processors over and above those included in the list of names referred to in Annex GDPR 5, it must request prior authorization from the Controller for such appointments, as per the attached standard (Annex GDPR 6). The latter reserves the right to issue a general authorization valid for the entire duration of the Contract or specific authorization depending on the nature of the service and the duties defined forth in Article 28 of the GDPR.

17.2.6.7. The Supplier declares that the Other Processors will process personal data in countries belonging to the European Union or countries that ensure suitable protection of personal data under the GDPR. The Supplier undertakes to provide details, specifying the location (region and town), of its Data Centres where personal data will be processed by Other Processors.

17.2.6.8. If Other Processors process data in the United States, if subject to US law, the Supplier is obliged to ensure the validity of Privacy Shield certifications or other certifications required by the Adequacy Decisions of US legislation on the part of the European Commission .

17.2.6.9. If an Other Processor belong to the Supplier's multinational group which has adopted the binding corporate rules pursuant to Article 47 of the GDPR, these constitute adequate assurances with regard only to that Other Processor.

Should the Sub-processors intend to process the personal data in countries considered inadequate in relation to the GDPR, the Supplier undertakes to have the Sub-processor sign the standard contract clauses defined by the decision of the European Commission in force at the time when this Contract is established. To this end, the Controller confers to the Supplier, as Data Processor established in the European Union, a specific mandate with representation so that it can sign the above-mentioned Standard Contract Clauses.

18. ETHICAL CLAUSES.

In addition to the provisions of art. "ETHICAL CONDUCT RULES." of the General Part

a. **General information**.
In activities carried on and relationship management, ENEL Group is guided by the principles contained in its Code of Ethics, Zero Tolerance Plan, the Organization Model, the Enel Global Compliance Program, available at http://www.ENEL.com. In the course of its own business and in managing its relationships with third parties, the Contractor declares that it shall be governed by equivalent principles; otherwise, ENEL reserves the right to terminate the agreement in compliance with the provisions of the Special Conditions.

The principles of health and safety vision of ENEL and of Stop Work Policy can be found at the following address: www.ENELdistributie.ro / www.ENEL.ro

b. **The Statement regarding the Conflict of interests.**
Regarding the obligations taken in compliance with art. "CONFLICT OF INTEREST" of the General Part, the Contractor undertakes to provide ENEL the statement referred to in Annex 1 to Annex Romania of this document, duly signed at the conclusion date of this agreement.

c. **Confidentiality declaration and regulations regarding the use of information systems of ENEL[2].**
The Contractor undertakes to comply with the obligations provided in Annex 2 of Annex Romania of this document. It also undertakes to provide ENEL with the statements listed in Annexachment, duly signed at the conclusion date of this agreement.

18.1 Integrity clause.
With the bid submission and /or the acceptance of the Contract, the Contractor[3] declares:

- To take note of the commitments made by ENEL S.p.A. and by the Companies it controls directly or indirectly (hereinafter "ENEL"), in the Code of Ethics, Zero Tolerance of Corruption (ZTC) Plan, Human Rights Policy, to respect equivalent principles in the conduct of its business and in managing relationships with third parties;

- [4]To be unaware of subjection to criminal proceedings for tax crimes, crimes against the public administration, crimes against patrimony, crimes against personal freedom, public order, environmental crimes;

- [5]To not be subjected to criminal investigations in respect of any fact, matter, unlawful criminal conduct constituting tax crimes, crimes against public administration, crimes against patrimony, crimes against personal freedom, public order, environmental crimes;

- To take note and authorize that - for the purposes of evaluation of the professional conduct of the itself and of the Company concerned, in accordance with the second and the third bullet of the present letter a) - ENEL may autonomously acquire more information, in any time, in consideration of the necessary existence of fiduciary duties with the Company involved.

The Contractor undertakes to promptly inform and provide any relevant documentation to ENEL:

1) In the case of acknowledge of subjection to criminal proceedings referred to in the second bullet of the previous letter a);

2) In the case of subjection to criminal investigation referred to in the third bullet of the previous letter a).

ENEL reserves its right to analyze at its sole discretion the above-mentioned information, for the purposes of assessment of the professional conduct of the Contractor itself and of the Company concerned.

19. SETTLEMENT OF LITIGATION.

19.1 Referring to Article "JURISDICTION" of the General Part, ENEL and the Contractor shall make every effort to resolve amicably by direct negotiations, any disagreement or dispute which may arise between them within or in connection with this Agreement/FA.

19.2 If, after 15 days from the commencement of these negotiations, ENEL and the Contractor are unable to settle amicably a contract dispute, any of the parties can request that the dispute be settled by the competent court in Bucharest/Timişoara/Constanţa (as the case may be) under the conditions of the law, in compliance with pre-court procedures, where appropriate.

---

[2] This provision applies to Agreements providing access to offices of ENEL and/or access and processing of data and information of ENEL Group, and the use by the Contractor, of the information systems of ENEL.

[3] The Legal Representative of the Company **on his/her own behalf, on behalf of** (a) the holder and the technical director, in the case of an individual company; (b) the associates and the technical director, whether it is a general partnership; (c) the associated partners and the technical director, if it is a limited partnership; (d) the managers with power of representation and the technical director and the sole shareholder natural person, or majority shareholder in the case of companies with less than four members, whether it is another type of company or consortium**, from the Company where their position is carried out and,** if applicable**, on behalf of the Parent Company and of** (e) holder and the technical director, in the case of an individual company; (f) the associates and the technical director, whether it is a general partnership; (g) the associated partners and the technical director, if it is a limited partnership; (h) the managers with power of representation and the technical director and the sole shareholder natural person, or majority shareholder in the case of companies with less than four members, whether it is another type of company or consortium, **from the Parent Company**.

[4] For itself and for the persons listed in note 3.

[5] For itself and for the persons listed in note 3.

20. INFORMATION AND DATA REGARDING THE PERFORMANCE OF THE AGREEMENT.

ENEL, at the request of the Contractor, shall provide all data necessary for the performance of the Agreement/FA. In case that data supplied by ENEL, are not sufficient or are incomplete, the Contractor has the obligation to request the necessary data in a timely manner. In the absence of such request, ENEL shall not be in any way responsible for the failure to comply with the provisions of the Agreement/FA.

21. PARTIAL INVALIDATION.

If one or several provisions of the Agreement/FA shall be considered by a court, government, regulatory or administrative entity or by any other competent jurisdiction, invalid or unenforceable, the invalidation or non-performance of that provision shall not affect the other provisions of the Agreement/FA and all provisions not affected by such invalidity or non- performance shall remain in full force and effect. The Parties agree to attempt to replace the invalid or unenforceable provision with a valid and enforceable provision to satisfy as much as possible the economic, legal and commercial aspects of the invalid or unenforceable provision.

22. LAW APPLICABLE TO THE AGREEMENT/FA.

Taking into account the provisions of art. “APPLICABLE LAW” of the General Part, the Agreement/FA shall be construed in accordance with the laws of Romania.

Annex no. 1

STATEMENT[1]

regarding conflict of interests

The undersigned ..... true and lawful attorney of _____ _____ ,

(denomination/name and location/ address) acting as ..... of the contract for ..... . declare that I do not have as members in the Board of Directors/management or supervisory body and/or shareholders or associates which are my husband/wife or close relatives to the fourth degree or in business relationships trade with people who hold decision-making positions within the contracting authority.

I, the undersigned, declare that the information provided are complete and true in every detail and I understand that ENEL has the right to ask, for verification and confirmation of statements, any supporting documents I have.

I understand that if this statement is not consistent with reality I am liable for violation of criminal law regarding false statements.

This declaration is valid for the entire period of contract performance.

Date of filling in .....

(capacity of the signatory party),

_____

(authorized signature)

[1] To be issued by the manager of the company/legal representative/ persons from the company's upper management

Annex no. 2

REGARDING the SAFETY OF USING THE INFORMATION SYSTEMS OF ENEL

CONFIDENTIALITY STATEMENT[1]

AGREEMENT no. ..... as of .....

OBJECT: *.....*

The undersigned:

_____

(name and surname of the informant)

☐ Individual (check only if the respective Agreement is not concluded with a Company)

(to be filled in only if the respective Agreement is concluded with a Company)

☐ Owner

☐ True and lawful attorney

of _____

(Name/Headquarters of the Company)

DECLARES:

- the list of all authorized persons, who in connection with the Agreement, have the right to enter the premises of ENEL and/or to access data and information on ENEL Group is composed of:

  1) Mr/Mrs.....

  (Name, Surname)

  2) Mr/Mrs.....

  (Name, Surname)

- that each of the above persons signed the specific individual confidentiality clause, attached to this statement;
- that the person responsible to keep the list above updated is:

  Mr/Mrs_____ email_____ Phone_____ Fax_____

Attached no.___ clauses of individual confidentiality

Date _____

Informant

.....

Signature and stamp

[1] To be issued by the manager of the company/legal representative/ persons from the company's upper management

INDIVIDUAL CONFIDENTIALITY STATEMENT[1]

AGREEMENT no. …… **AS OF** ……

OBJECT: ……

The undersigned ……

Born in ..... (.....), on ……

(To be filled in only if the respective Agreement is concluded with a Company)

☐ employee
☐ consultant
} of Company ……

Regarding the related Agreement, he/she undertakes:

- not disseminate or disclose to third parties the information collected, opinions, studies, and other elements that could be provided by ENEL to perform the related Agreement and use this information only for the purposes of this Agreement, except where the undersigned must comply with legal obligations or requirements of public authorities to which he/she cannot legally refuse to fulfil;
- regularly inspect and comply with the security requirements regarding the data provided in the Annex, in case he/she possibly uses the systems made available by ENEL and store with maximum care all the documents on paper and/or electronically, obtained or produced during the performance of activities.

The information disclosed by ENEL or resulting from public official documents are excluded from the scope of confidentiality obligations.

The confidentiality obligations are fixed for a period of 5 years **from the expiry of this commitment, even in the event of cessation and termination, direct or indirect of the contractual relationship with ENEL.**

For acceptance

Signature

Date: ……

[1] To be issued by the persons mentioned in the Confidentiality Statement list, issued by the Company

Security instructions for the use of information systems of ENEL

All data, information and information systems provided by the ENEL Group are the property of the company and their use will be made only with the approval of ENEL.

Access to data, information and information systems owned by ENEL Group and their use should be implemented in accordance with safety regulations below:

- access will be granted only after signing certain confidentiality clauses, strictly to fulfil the tasks and activities covered by the contract for a limited time. The limited period of time allowed for access will not exceed the contract's validity period.
- access is made by compliance with ENEL policies, rules and procedures, regarding information security, legal framework in force and the right to privacy of other colleagues;
- access is made by ensuring the principles of integrity, availability and confidentiality of data, information and information systems;
- the access key to ENEL information systems must be used exclusively used by the staff and only for the fulfilment of work tasks. The password must be kept confidential and changed at least every 60 days or whenever there is a suspicion of being compromised. If using other authentication mechanisms, they must be used and held in maximum security.
- the users of access rights are responsible for the use method of the information resources and for the actions which may damage the security of information resources;
- the users of access rights, by their actions, must not try to compromise the protection of information systems and must not perform actions affecting the privacy, integrity or availability of any type of information;
- depending on the risk degree, access to data, information and information systems is monitored. ENEL reserves the right to review daily, or from time to time, logs containing relevant security events of the information describing the actions of the users of access rights.
- when they provide or discover non-compliance with IT security measures, IT security breaches, possible vulnerabilities, risks or threats to information systems, users are required to report these to the Security Department, who will investigate and act accordingly.
- the level of the right of access to the information system should be limited to the components necessary for carrying out the activities covered by the contract. Even if the granted level of access allows access to other components that are not needed, access must be used in good faith;
- access rights, equipment and information systems should not be used to connect to the Internet or other open networks, other than those that may be provided by ENEL;
- equipment not provided by ENEL and needed for the performance of contractual activities, may be connected in the ENEL network only if access is granted (at least by e-mail). The configuration of these devices must comply with the information security policy and have implemented updated IT security measures to prevent the programs such as virus, Trojan, worms and other malicious or illicit programs that can cause failures to ENEL computer service
- the users of access rights should not handle the data and information in electronic format which contravenes laws, which contain racist, abusive, discriminatory, pornographic, paedophile, racist content, content inciting to the use of prohibited substance, war crimes, crimes against humanity , rape, murder, violence, or pirated software or pirated media files that can harm the ENEL Group.

In compliance with the requirements above, ENEL reserves the right to prohibit the improper use of its IT infrastructure, without prejudice the compliance with the provisions of legislation in force. Nevertheless, ENEL also reserves the right to notify the competent judicial authorities on any possible infringement of regulations which might be considered an offense.

Attachment GDPR

Attachment 1 GDPR

Data Processing Description

With reference to paragraph 17 of Annex Romania and to the order letter n. ..... and in particular to the appointment of the company ..... as Processor, by this attachment the Controller means to identify types of data and categories of data subjects related to the above mentioned Contract.

A. Type of personal Data

- Biographical Data[1] □
- Special Categories of Personal Data[2] □
- Personal Economic & Financial Data □
- Judicial Data □
- Others _____

_____
_____
_____

B. Data Subjects Categories

- Customers □
- Employees □
- Contractors □
- Others _____

_____
_____
_____

Full name of the Processor's legal representative
Position
Name of the Processor
Date
Signature

[1] E.g.. name, surname, home address, credit card number, Identity Card number, Passport number, IP (Internet Protocol); address, geolocalization data

[2] Including sensitive data, e.g. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.

Attachment 2 GDPR

Dear NAME AND SURNAME Authorized Person

RE. CONTRACT N ._____

Subject:

- **TEMPLATE: APPOINTMENT AS AUTHORIZED PERSON FOR PROCESSING PERSONAL DATA (HEREAFTER "AUTHORIZED PERSON"), PURSUANT TO ARTICLE 29 OF EU REGULATION 2016/679 (HEREAFTER "GDPR ")**

The Processor, warrants that it informed the

The xxxxxx Company, as the processor of personal data under the Contract referred to above

WHEREAS:

The performance of activities related to your contractual duties / qualification implies processing personal data and requires, among other things, in relation to the above-mentioned Contract, access to the ENEL Company's IT systems ……, the Data Controller of the personal data processing in question;

To this end, you must be accredited for these systems.
The foregoing processing and the foregoing authorization assume your appointment as an "*Authorized Person*" for processing personal data under the direct authority of the Data Controller pursuant to Article 29 of the GDPR

INASMUCH, IT IS HEREBY AGREED AS FOLLOWS

the undersigned Company

APPOINTS

Mr. xxxx, born in xxxx on xxxx. Tax Code xxxxx, as **Authorized Person** for processing personal data, that is for any operation, even if only for consultation, relating to personal data stored in IT and/or paper files held by the undersigned Company and/or by the Company [•], Data Controller, associated with performing the tasks related to your duties/qualification _____, c/o head offices in _____.

Information and minimum instructions are provided below for the performance of the tasks assigned both to the Processor and to the above mentioned Authorized Persons, you in relation to processing personal data processed within IT systems/application and/or in paper files.

In particular, it is hereby specified that:

- Processing of personal data must be carried out in a lawful and correct manner;
- Personal data must be collected and recorded solely for purposes associated with the activity carried out, exclusively during working hours and in any case for no longer than the necessary time;
- Without prejudice to the foregoing, in the exceptional case of personal data processing performed outside working hours, the Authorized Person must ensure that he/she has closed the work session ("log-off") so that access credentials are requested for the next session;
- Constant verification of data and their updating is necessary;
- Constant verification of the completeness and relevance of processed data is necessary;
- Any consensus collection stage must be preceded by a specific notification and the issue of consent by the data subjects, which must be free, specific and in writing or otherwise specifically documented;
- In the event of interruption, even temporary, of work you must make sure that already processed data are not accessible to unauthorized third parties by implementing a specific log-off;
- Your authentication credentials must be confidential and as such exclusively used by the Authorized Person;
- Maximum confidentiality must be assured for every data processing operation.

In particular you, as an Authorized Person, are required to:

a) access only personal data the knowledge of which is strictly necessary to fulfil the tasks assigned and for no longer than the time necessary;

b) not leave unguarded or exposed to the view of subjects not involved in the processing, corporate documents with particular reference to those containing sensitive and legal data, ensure the necessary confidentiality of the data in question, taking appropriate precautions - also on the basis of instructions from the Data Controller - to prevent unauthorised subjects from accessing the said data;

c) not disseminate or communicate data coming into your possession, except in cases permitted by law or provided for by contractual regulations, and maintain due reserve with regard to information that you have become aware of during your appointment or even when the appointment is no longer in effect;

d) not download massive amounts of personal data without the prior communication to and authorisation of the Data Controller or Processor;

e) in any case, with appropriate care and due diligence store the hard copies of documents entrusted for the implementation of your work which contain sensitive data and data concerning criminal records, in cabinets or drawers provided with locks and observe the relevant procedure (indication in the relevant register of your name, time and date of access, removal/return of the document) for accessing files containing the above mentioned data;

f) adopt and scrupulously follow the instructions of the Data Controller and/or Processor with regard to appropriate organisational and technical measures that ensure a level of security adequate to the risk (pursuant to Art. 32 GDPR);

g) in particular, for processing data with electronic or automated devices, observe any specific authorisations/qualifications and the methods and conservation tools provided by the Data Controller and/or data processor;

h) inform the Manager in the event of incidents involving the personal data being processed, in particular if sensitive and/or judicial.

In any case, it is your responsibility to comply scrupulously with the **dispositions concerning suitable security measures as per Article 32 of the GDPR**, listed at the end of this document and forming an integral part of it, which you declare to have read, as well as any additional dispositions that may be required by the undersigned Company and/or the Data Controller, updates of which will be communicated to you.

Lastly, the following items should also be noted:

- this letter of appointment will cease to be effective on the date of termination of the employment relationship or the appointment with the undersigned company; consequently, after that date any processing of personal data, including access to the IT systems of the undersigned Company and/or Data Controller, is prohibited and subject to sanctions in accordance with the current dispositions of the Romanian law (see, by way of example, Romanian Criminal Code concerning "*Unauthorized access to IT or telecommunications systems*");

- a copy of this letter will be returned by the Authorized Person to the undersigned Company, signed by way of acknowledgement and acceptance, and will be kept by said Company and made available to the Data Controller, if expressly so requested, no later than two days from the request itself;

- to avoid any unauthorized data processing, the undersigned Company will inform the Data controller of the termination of the employment relationship or the assignment in place no later than five days from the event, so that the Data Controller can arrange immediate revocation of the IT authorizations it issued.

Full name of the Processor's legal representative
Position
Name of the Processor
Date
Signature

_____

By way of acknowledgement and acceptance - Authorized Person

_____

INSTRUCTIONS FOR "PERSONS AUTHORISED" TO PROCESS PERSONAL DATA

EU Regulation 2016/679 concerning the protection of personal data (hereinafter "GDPR") requires all those who process personal data to carry out operations with respect for and protection of the natural persons to which the data refer, whether they are employees, suppliers of goods and services, customers, consultants, etc.

The GDPR specifically envisages the need to provide adequate instructions for all those who, in relation to the implementation of their work, process personal data; in other words, those who use or become aware of personal data as described in Art. 4 No. 1 of the GDPR (see definitions at the end).

In compliance with the provisions of the GDPR, as "Authorised Person" you shall process the relevant personal data by paying scrupulous attention to the following instructions and to all other instructions that may be provided by your data processor or the Data Controller or other person delegated by it.

Please remember that the personal data must be processed:
- in observance of the criteria of confidentiality;
- lawfully and correctly;
- for a period of time not exceeding that necessary for the purpose for which the data have been collected or subsequently processed;
- with total observance of suitable security measures, by storing and controlling the data subject of the processing in such a way as to avoid the risk, even accidental, of destruction or loss, of unauthorised access or processing that is not permitted or does comply with the purpose of the collection.

In particular, with regard to:

- **Access to personal data**, data banks and corporate applications: data, data banks and corporate applications you may access are those that are strictly indispensable for the implementation of your work, in line with your role and, as far as regards IT applications, in accordance with the user profile assigned to you.
- **Creation of new procedures/applications**: without prior authorisation, you cannot activate new IT procedures for the management or processing of data, files including hard copies, or personal data files. If the above is necessary, you must give your immediate superior prior notice and proceed only after receiving authorisation.
- **Communication and dissemination**: the data you have access to during your work must be processed by you personally, or by your colleagues, but cannot be communicated and/or transmitted to outside third parties.
- **Security measures**: it is your responsibility to observe all current protection and security measures aimed at preventing the risk of destruction, loss, unauthorised access or prohibited processing; in particular, your password must not be given to anyone, your PC must not remain connected to company files and accessible in your absence; hard copies of data must be placed in locked cabinets at the end of the day and always after being used; in any case, you must assure the confidentially of hard copies of data every time you leave your workstation. All episodes that you deem important as regards data security must be immediately communicated to your Manager. Special attention must be paid to the management of documents containing data of a juridical and/or sensitive nature.
- **Requests for access/exercise of rights**: if you receive a request to access personal data ex Chapter 3 “Rights of data subject” of the GDPR, from the data subject (whether it is an employee of the company, a supplier, a customer, a consultant, etc.), you must take note of the same in writing, specifying the date and the name of the data subject, and immediately refer the same to your Manager or to the relevant organisation office, which will respond within the established time frame.

1. PROCESSING WITHOUT ELECTRONIC DEVICES

Personal data filed on magnetic and/or optical media must be protected by the same security measures as those adopted for hard copies.
The security measures applied to copies or reproductions of documents containing personal data must be identical to those applied to the originals

1.1 Safekeeping

Documents containing personal data must be stored in such a way that they are not accessible by persons not authorised to process them (e.g.: cabinets or drawers that can, if possible, be locked).
Documents containing personal data that are removed from the files for day-to-day work must be returned at the end of the day.
Documents containing personal data must not be left unattended on desks or work tables; similar attention must be paid when removing documents that have been received via fax; as a general rule you should avoid printing documents unless it is strictly necessary and in any case they must be removed immediately so that they are not left unattended at the printer.

1.2 Communications

The use of personal data must take place on the basis of the “need to know” principle and they must not be shared, communicated or sent to persons who do not require them for the implementation of their work (even if such persons are also authorised to process data). Data must not be disclosed outside the Company and in any case to third parties unless authorized by the Data Controller or the Data Processor.

1.3 Destruction

If it is necessary to destroy documents containing personal data, they must be destroyed by using the appropriate shredders or, in their absence, they must be cut into small pieces so that they cannot be reassembled.
Magnetic or optical media containing personal data must be erased before they can be reused. If this is not possible, they must be destroyed.

1.4 Additional instructions for processing sensitive and judicial data

Documents containing sensitive and/or judicial data must be controlled and stored by Authorised Persons in such a way that they cannot be accessed by unauthorised persons. For example, reference to documents/certificates for insertion in electronic personnel management/administration procedures, data regarding trade union authorisations, sick leave, etc., must take place in the time strictly necessary for keying in the same and, immediately after, the documents must be filed in accordance with these instructions. The filing of hard copies containing sensitive and/or judicial data must be kept separate from those concerning common data (the same cabinet or drawer may be used - and possibly locked - but the containers must be separate).
To access files containing sensitive or judicial data outside office hours you must be identified and recorded in the relevant registers.

2. PROCESSING WITH ELECTRONIC DEVICES

2.1 Management of authentication credentials

The law envisages that access to electronic procedures that process personal data is permitted by Authorised Persons in possession of “authentication credentials” which allow them to bypass an identification procedure. Authentication credentials consist of a code for identifying the Authorised Person for processing personal data (user-ID) associated with a confidential password, or an authentication device (e.g.: smart card, token, one-time-pw), or a biometric characteristic. Authorised Persons must use and manage their authentication credentials in accordance with the following instructions.

Individual user-IDs for accessing applications must never be shared amongst users (even if Authorised Persons for data processing). If other users must access data, they are required to request authorisation from their Manager.
Authentication credentials (for example passwords or strong authentication devices like tokens, smart cards, etc.) that allow access to applications must be kept confidential. They must never be shared with other users (even if Authorised Persons for data processing).
Passwords must be changed by the Authorised Person following the first use and subsequently, in observance of the specific corporate procedures, at least every three months in the case of sensitive and judicial data processing, or at least every six months for personal/shared data.
Passwords must consist of at least eight characters or, if this is not permitted by the electronic device, by the maximum number of characters permitted. Passwords must not contain references that easily lead to the Authorised Person (e.g.: family names) and must be chosen in accordance with corporate regulations concerning the construction and use of passwords (see also point 3, below), unless more restrictive instructions are envisaged by corporate systems.

2.2 Protection of PC and data
All PCs must have passwords that comply with the instructions given in the next point below. Passwords must be kept and managed with due diligence and in observance of the instructions provided by the Data Controller or, on its behalf, by the Processor.
To prevent illicit access, the screen saver password must always be activated if this setting is not automatically available.
As soon as they are available (and in any case at least annually) all software updates necessary for preventing vulnerability and correcting defects must be installed in the PCs. If this does not take place automatically, the Authorised Person must inform his/her Manager.
Back-up storage must be carried out at least every week on the assumption that any third party personal data are present only in the PC of the Authorised Person (not filed in corporate IT systems). The storage media used for back-up must be managed in accordance with the rules described in “Processing without electronic devices”.
2.3 Deletion of personal data
In the event of disposal of work tools, it is your responsibility to eliminate all personal data they contain.
2.4 Additional instructions for processing sensitive and judicial data
Passwords for accessing IT procedures used to process sensitive and judicial data must changed, by the Authorised Person if an automated system is not available, at least every three months, unless more restrictive methods and time frames are communicated from time to time by the Manager or provided for in procedures.
The installation of software updates required to prevent vulnerability and correct computer program defects must be carried out at least every six months if an automated system is not available.

3. GENERAL INSTRUCTIONS

<u>How to choose and use a password</u>
- Use at least 8 characters
- Use letters, numbers and at least one character from . ; $! @ - > <
- Do not use your own or a relative's date of birth, name or surname
- Do not use a matriculation number or user ID
- Always keep it in a safe place that cannot be accessed by third parties
- Do not divulge it to third parties
- Do not share it with other users

<u>Conduct in the presence of guests or service personnel</u>
- Have guests wait in places where confidential information or personal data are not present.
- If necessary, move away from your desk when guests are present, put documents away and enable the PC screen saver by pressing “ctrl-alt-del” on the keyboard and selecting “Lock Computer”.
- Do not reveal passwords to technical assistance personnel and/or allow them to type in passwords.
- Do not reveal passwords over the telephone - no one is authorised to request them.

<u>How to handle e-mails</u>
- Do not open messages with attachments if you do not know the source since they could contain viruses that will delete or steal data stored in the PC.
- Avoid opening films, presentations, images and files in any format if they come from unknown sources since these could pose a threat to the data contained in your PC and, in general, to the security of the corporate technological infrastructure.
- Avoid forwarding automatically from your company mail box to external personal mail boxes and vice-versa.

<u>How to use the Internet correctly</u>

- Avoid downloading software from the Internet (utility programs, office automation, multimedia files, etc.) as these could pose a threat to the data and the company network, unless the software is required for the implementation of your work and its use is in any case known to the relevant corporate organisation offices.

4. PENALTIES FOR NON OBSERVANCE OF REGULATIONS

You are reminded that the use for personal purposes or in any case for unlawful aims of the data to which you have access or have accessed, even if it does not cause damage to and/or responsibility for the Controller, according to applicable Romanian law (Civil Code, Criminal Code etc.), could in any case be subject to the application of disciplinary or criminal penalties, as this could be construed as a breach of the duties that are incumbent on the employee, as envisaged by the Romanian Labour Code or by the applicable Collective or Individual Labour Agreement.
You are requested to promptly report any evidence of situations that put the security of data at risk (e.g.: password breach, attempted unauthorised access to the systems) or which concern external subjects authorised to access (obvious breach of corporate Procedures): your collaboration is important for closing any gaps in the security systems and procedures for protecting the personal data processed.
These instructions are the guidelines to be followed for your work: inasmuch, if in doubt, please contact the Manager.

5. DEFINITIONS

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.
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, cultural or social identity of that natural person;
Special categories of data: personal data that reveal racial or ethnic origins, political opinions, religious or philosophical beliefs or trade union membership, as well as biometric data intended to unequivocally identify a natural person, data concerning the health or sexual history or orientation of the natural person (Ed: disabilities, medical certificate, indication of illnesses/accidents, handicaps, etc.).
Judicial data: personal data that will reveal criminal convictions and offenses or to other related security measures with regard to criminal records, the register of crime-related administrative penalties and the relevant pending charges, or the status of the accused or suspect pursuant Romanian Code of Criminal Procedure and Criminal Code (e.g.: imprisonment or house arrest, legal disqualification, provisions relating to amnesty and pardon, etc.).
Data controller: the 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;
Processor: the natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller;
Authorized Person for data processing: Person authorized to process personal data under the direct authority of the Data Controller or the Data Processor.
Data subject: the natural person to whom the personal data refer (e.g.: employees, customers, suppliers, visitors, etc.).
Security measures: All the technical and organisational measures that adequately guarantee a level of security adequate to the risk (Ed: pseudonymisation, encryption, user id, password, use of containers with locks, etc.).
Personal data breach: means 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.

Attachment 3 GDPR

Appointment as Authorized Person for Processing Personal Data (hereafter "Authorized Person"), pursuant to Article 29 of EU Regulation 2016/679 (hereafter "GDPR ")
SUBSTITUTIVE DECLARATION

Messrs ……

The undersigned .....
(surname) (name)……
born in ..... (.....), on ……
(place) ..... (prov.) .....
resident in …… (…….) Address …… n. ……
(place)…….. (province.)…… (address)……
domiciled in ..... (.....) in Address ..... n. ……
(place)…….. (province…… (address)……
……
as legal representative of the Firm / Company .....
with registered head offices in ..... (.....) Address ..... n. ...
Tax Code ……..VAT n. ……

as Data Processor, aware of the penal sanctions referred to in the Romanian Criminal Code – chapter VI - as regards false declarations and the creation or use of false documents, under his/her own responsibility

DECLARES

- having appointed employees/collaborators in relation to the activities referred to in the above-mentioned contract as **"Authorized Persons"** for processing personal data as per Article 29 of the GDPR using the template appointment letter prepared by you including the related Instructions
- that a copy of these appointments in his/her possession is available and at the disposition of the Processor

HEREBY ATTACHES

- to this document the list of names of persons appointed as Authorized persons

UNDERTAKES

- to provide to the Controller with a copy of appointed persons by the date that will be specifically nominated by the Processor;
- to update the documentation sent, before starting activities in the case of new employees/collaborators or within 5 (five) working days from the date of termination when employees/collaborators are no longer involved.

Full name of the Processor's legal representative
Position
Name of the Processor
Date
Signature

Privacy notice pursuant to Article 13 of the GDPR

We hereby inform you that personal data are acquired with this Annex and are processed for purposes strictly related to the management and execution of the Contract or to implement obligations required by law. Additionally, personal data will be collected and processed using automated means and in paper form and will be stored for the entire duration of the Contract and after its termination for a period not exceeding the terms envisaged by applicable laws.

In this respect, it should be noted that:

– the Data Controller for the data in question is the the following Enel Company …… (hereinafter "*Controller*");

- The data subject is the natural person whose personal data are processed for the purposes of stipulation, management and execution of the Contract (hereinafter the "*Data subject*");
- The personal data processed may be transmitted to third parties, i.e. to companies subject to management and coordination by ENEL S.p.A. or connected with ENEL, or to other subjects. These third parties may be appointed as Data Processors;
- The data subject is entitled to exercise the rights envisaged in Articles 15-21 of the GDPR (right to access data, request their rectification, portability or cancellation, request the limitation of processing of data concerning him/her or may oppose processing), where applicable, by contacting the Data Controller;
- The data subject is entitled to lodge a complaint to the Romanian Data Protection Authority (ANSPDCP), with registered office in Bucuresti, B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, cod postal 010336, Romania, Tel. (+40) 318059211 or (+40) 318059212, email: anspdcp@dataprotection.ro;;
- The Data Controller has appointed the Data Protection Officer (DPO) pursuant to Article 37 of the GDPR, whose contact details can be found on the Data Controller's website.

N.B. The signature of the owner or legal representative must be accompanied by non-authenticated photocopy of the signer's identity document (front/rear)

Attachment 4 GDPR

Appointment of the Other Processor by the Data Processor

REF. CONTRACT N ._____

Messrs
Company name of the Supplier
.....

Subject: **APPOINTMENT AS OTHER PROCESSOR FOR PROCESSING PERSONAL DATA (HEREAFTER "OTHER PROCESSOR"), PURSUANT TO ARTICLE 28, PARAGRAPH 4 OF EU REGULATION 2016/679 (HEREAFTER "GDPR")**

1. In relation to the above-mentioned contract, the Enel Company [•], in its capacity as Data Controller for the data managed in relation to said contract (hereafter also "ENEL"), has appointed, pursuant to and for the purposes of Article 28 of EU Regulation 2016/679 ("GDPR"), the Company _____with registered office _____ address _____ as data processor (hereafter "Processor").
2. The legal representative of the Processor, intends to make use for specific processing activities of a subject external to its own organization, having obtained the authorization of ENEL to proceed in this manner.

Inasmuch, it is hereby agreed as follows

the legal representative, in the person of _____ in his/her capacity as _____ **appoints** the Company _____ with head offices in _____ address _____ as Other Processor for processing data pursuant to Article 28, paragraph 4 of the GDPR (hereafter "*Other Processor*") limited to those operations necessary to implement the Contract referred to the object to which reference is made - as an integral part of this letter - to define the scope and time period to which the responsibility for processing personal data refers.

The Other Processor undertakes to perform said operations in accordance with the obligations imposed by the GDPR on the Processor and the instructions issued by the Data Controller, who will ensure strict compliance with them.
In particular, whereas the Other Processor, in relation to its declared experience, capacity and reliability, has provided a suitable guarantee of full compliance with the applicable data processing regulations, and in line with the new European Community GDPR law, its duties and responsibilities are defined, by way of example, as follows:

o) They must only process the personal data when instructed to do so by ENEL, registered in a document in which the type of data processed and the categories of Data Subjects are listed;
p) They will have to appoint Authorized Persons for processing personal data ("Authorized Persons") to carry out of any operation, including simple consultation, concerning processing personal data entered in IT or paper files held by ENEL;
q) They must ensure that the Authorized Persons for processing personal data have undertaken to observe legal dispositions as well as every indication of Enel and also maintain the confidentiality of the , information and personal data coming to their knowledge as a consequence or even only during the execution of the Contract and not to communicate them to third parties, unless expressly authorised to do so by ENEL and except for the cases expressly envisaged by law; ENEL reserves the right to request the Supplier to provide the list of Authorized Persons for data processing in order to comply with obligations under the GDPR or other legal requirements or for reasons of national security or public interest;
r) They must adopt all the security measures as set forth in Article 32 of the GDPR, as well as all other preventative measures dictated by the experience designed to prevent any processing of data that is not allowed or not compliant with the purposes for which the data are processed; they must also ensure that they collaborate effectively in implementing these measures, in notifying and communicating any breaches of the personal data and in assessing the impact on the data protection in order to ensure the confidentiality and security of the data and minimise the risks that the data in question might be accidentally destroyed or lost;

s) On express request by ENEL, they will have to provide the list of countries and data centres where personal data are processed on behalf of ENEL;

t) They may transfer the data to a third country or to an international organisation located outside the European Union only in cases envisaged and under the conditions defined by the GDPR, unless this is required by the law of the European Union or the national law to which the Supplier is subject. In this case, the Supplier undertakes to inform promptly ENEL about this legal obligation unless forbidden from doing so for relevant reasons of national security or public interest;

u) Bearing in mind the nature of the processing, the Supplier undertakes to help ENEL with its own appropriate technical and organisational measures, to the extent to which this is possible, with a view to fulfilling the duty of the latter to act on the data subject's request to exercise their rights;

v) It must assist ENEL in ensuring compliance with the duties set forth in Articles 32 to 36 of the GDPR, in consideration of the nature of the processing and the information available;

w) They must, on ENEL's request, erase and/or return all the personal data once the execution of the services relative to the processing have been completed and erase the existing copies, unless the law of the European Union or its member States envisages that the data be stored, providing ENEL with proof that this has been accomplished;

x) When a Data Protection Officer has been appointed pursuant to Article 37 of the GDPR, this must be communicated to ENEL;

y) They must provide ENEL with all the information necessary to demonstrate compliance with the requirements of the GDPR by participating in the review activities, including the inspections, carried out by ENEL or by another party appointed by the same;

z) In case of actual or suspected personal data breaches, they must promptly notify ENEL within 24 hours of becoming aware of the event and without any unjustified delay;

aa) They must cooperate with ENEL by making freely available all necessary information in order to fulfil the obligations defined in Articles.33 and 34 of the GDPR, including current certifications;

bb) Over and above the dispositions of Article 30, item 5 of the GDPR, they must keep a register of the processing activities carried out on behalf of ENEL pursuant to Article 30 of the GDPR, which must be exhibited on the request of ENEL, if applicable, in case of events which are regulated by Articles 33 and 34 of the GDPR.

The Other Data Processors must comply with the obligations that this Contract imposes on data processors.
The Other Processor in turn will appoint any resources used in data processing as Authorized Persons for processing personal data, using the appropriate template prepared by the Data Controller attached herein (Annex GDPR 7).
By the date that specifically notified by the Data Controller, and in any case before the start of activities detailed in this contract, the Other Processor will also send a declaration using the template prepared by the Data Controller (Annex GDPR 8).
Annex GDPR 8, in digitally signed pdf format together with the list of persons authorized for data processing by the Other Processor (as per the template made available by the Data Controller), shall be sent to the Data Processor and the Data Controller in accordance with the indicated for this purpose.
In the same manner as indicated above, the Other Processor also undertakes to update the above-mentioned documentation in the event of any changes. In any case, updates will be sent before the start of activities for new employees/collaborators and within five working days from the date of termination for the employees/collaborators no longer involved.
Both the Processor and the Other Processor are obliged in any case to diligently archive the foregoing appointments and to make them available if requested by the Data Controller no later than two days from said request.
The Other Processor will process personal data in countries belonging to the European Union or in countries that ensure appropriate protection of personal data pursuant to the European Commission's Adequacy Decision.
If the Other Processor intends to process the Personal Data in countries not deemed adequate by the European Commission, the Processor shall ensure that the Sub-processor signs the standard contractual clauses defined by the European Commission decision in effect when this Contract is signed.

Compensation and liability
Anyone who may suffer material or immaterial damages caused by a breach of the duties specified in the GDPR is entitled to obtain compensation for the damage from the Data Controller or Data Supervisor.
Without prejudice to the Other Processor's duties to indemnify ENEL, as already envisaged in the Contract, he/she will in any case be liable for the damage caused by the processing if it has failed to comply with the duties as imposed by the Contract or has acted in a different or contrary way to the lawful instructions of the Data Controller.

System administrators
Since the Other Processor's personnel may perform functions within the qualification of "system administrator" in accordance with current legislation, the Other Processor undertakes to provide, at the request of the Processor or Data Controller, a list of collaborators, authorized and appointed as "system administrators", as well as all those who may potentially intervene on personal data owned by ENEL.
The Processor and Other Processor also undertake to keep a register of the logs of access, disconnection and attempted access of its collaborators and/or the collaborators of the Sub-managers, if authorised, who have been appointed as "system administrators" and who in such a capacity have the possibility of processing the personal data of which ENEL is Data Controller for a period of six months, with the commitment to submit them to the latter within 3 calendar days in the specified format, upon receipt of a request in writing from the Data Controller.

Duration
The foregoing appointment of the Other Processor will be automatically revoked at the end of the contractual relationship or on termination for any other reason whatsoever.

Please return the attached copy of this letter, signed by way of acceptance, and report hereafter every fact and matter of particular importance that may come to light in the application of current legislation.

Best regards,

Full name of the Processor's legal representative
Position
Name of the Processor
Date
Signature

_____

For acceptance

Full name of the Other Processor's legal representative
Position
Name of the Other Processor
Date
Signature

_____

Attachment 5 GDPR

COMPANY	COUNTRY AND ADDRESS	PRODUCT OR SERVICES	TYPE OR CATEGORY OF DATA PROCESSED	DATA ARE PROCESSED within the following EU / non-EU countries	PRIVACY SHIELD OR OTHER RELEVANT CERTIFICATIONS applicable for the data processing within non-EU countries

Attachment GDPR 6

RE. CONTRACT N ._____

Subject: REQUEST FOR AUTHORIZATION OF APPOINTMENT OF DEPUTY MANAGER PURSUANT TO ARTICLE 28 OF EU REGULATION 2016/679 (HEREAFTER "GDPR")

The Company xxxxxx, as Data Processor appointed by [•], as Data Controller

- WHEREAS:
-
-
- for the execution of specific processing activities related to the execution of the foregoing Contract, use must be made of subjects external to their own organization;
- for these purposes, pursuant to Article 28 of the GDPR, the Processor appointes ....., ... legal entity with registered office in ……., J……., Tax Identification Number ……..……..., represented by ……..… as ….....…., as Other Processor

(i)
INASMUCH, IT IS HEREBY AGREED AS FOLLOWS

The Company xxx requests [•], in its capacity as Data Controller, authorization to appoint the Company xxx as Other Processor using the template prepared by it and attached herein.

Full name of the Processor's legal representative
Position
Name of the Processor
Date
Signature

For acceptance

Full name of the Controller's legal representative
Position
Name of the Controller
Date
Signature

_____

Attachment GDPR 7

Dear NAME AND SURNAME Authorized Person

_____

RE. CONTRACT N ._____

Subject: TEMPLATE: APPOINTMENT AS AUTHORIZED PERSON FOR PROCESSING PERSONAL DATA (HEREAFTER "AUTHORIZED PERSON"), PURSUANT TO ARTICLE 29 OF EU REGULATION 2016/679 (HEREAFTER "GDPR ")

The xxxxxx Company, as the Sub-processor of personal data, authorized by Enel Company [•] as Data Controller under art. 28 GDPR

WHEREAS:

- The performance of activities related to your contractual duties / qualification implies processing personal data and requires, among other things, in relation to the above-mentioned Contract, access to the ENEL Company's IT systems [•], the Data Controller of the personal data processing in question;
- To this end, you must be accredited for these systems.

The foregoing processing and the foregoing authorization assume your appointment as an "Authorized Person" for processing personal data under the direct authority of the Data Controller or of the Data Processor pursuant to Article 29 of the GDPR

INASMUCH, IT IS HEREBY AGREED AS FOLLOWS

the undersigned Company

APPOINTS

Mr. xxxx, born in xxxx on xxxx. Tax Code xxxxx, as **Authorized Person** for processing personal data, that is for any operation, even if only for consultation, relating to personal data stored in IT and/or paper files held by the undersigned Company and/or by the Company [•], Data Controller, associated with performing the tasks related to your duties/qualification _____, c/o head offices in _____.

Information and minimum instructions are provided below for the performance of the tasks assigned both to the Processor and to the above mentioned Authorized Persons, you in relation to processing personal data processed within IT systems/application and/or in paper files.

In particular, it is hereby specified that:

- Processing of personal data must be carried out in a lawful and correct manner;
- Personal data must be collected and recorded solely for purposes associated with the activity carried out, exclusively during working hours and in any case for no longer than the necessary time;
- Without prejudice to the foregoing, in the exceptional case of personal data processing performed outside working hours, the Authorized Person must ensure that he/she has closed the work session ("log-off") so that access credentials are requested for the next session;
- Constant verification of data and their updating is necessary;
- Constant verification of the completeness and relevance of processed data is necessary;
- Any consensus collection stage must be preceded by a specific notification and the issue of consent by the data subjects, which must be free, specific and in writing or otherwise specifically documented;
- In the event of interruption, even temporary, of work you must make sure that already processed data are not accessible to unauthorized third parties by implementing a specific log-off;
- Your authentication credentials must be confidential and as such exclusively used by the Authorized Person;
- Maximum confidentiality must be assured for every data processing operation.

In particular you, as an Authorized Person, are required to:

b) access only personal data the knowledge of which is strictly necessary to fulfil the tasks assigned and for no longer than the time necessary;

b) not leave unguarded or exposed to the view of subjects not involved in the processing, corporate documents with particular reference to those containing sensitive and legal data, ensure the necessary confidentiality of the data in question, taking appropriate precautions - also on the basis of instructions from the Data Controller - to prevent unauthorised subjects from accessing the said data;

c) not disseminate or communicate data coming into your possession, except in cases permitted by law or provided for by contractual regulations, and maintain due reserve with regard to information that you have become aware of during your appointment or even when the appointment is no longer in effect;

d) not download massive amounts of personal data without the prior communication to and authorisation of the Data Controller or Data Processor;

e) in any case, with appropriate care and due diligence store the hard copies of documents entrusted for the implementation of your work which contain sensitive data and data concerning criminal records, in cabinets or drawers provided with locks and observe the relevant procedure (indication in the relevant register of your name, time and date of access, removal/return of the document) for accessing files containing the above mentioned data;

f) adopt and scrupulously follow the instructions of the Data Controller and/or Data Processor with regard to appropriate organisational and technical measures that ensure a level of security adequate to the risk (pursuant to Art. 32 GDPR);

g) in particular, for processing data with electronic or automated devices, observe any specific authorisations/qualifications and the methods and conservation tools provided by the Data Controller and/or data processor;

h) inform the Manager in the event of incidents involving the personal data being processed, in particular if sensitive and/or judicial.

In any case, it is your responsibility to comply scrupulously with the **dispositions concerning suitable security measures as per Article 32 of the GDPR**, listed at the end of this document and forming an integral part of it, which you declare to have read, as well as any additional dispositions that may be required by the undersigned Company and/or the Data Controller, updates of which will be communicated to you.

Lastly, the following items should also be noted:

- this letter of appointment will cease to be effective on the date of termination of the employment relationship or the appointment with the undersigned company; consequently, after that date any processing of personal data, including access to the IT systems of the undersigned Company and/or Data Controller, is prohibited and subject to sanctions in accordance with the current dispositions of the Romanian law (see, by way of example, Romanian Criminal Code law "*Unauthorized access to IT or telecommunications systems*");

- a copy of this letter will be returned by the Authorized Person to the undersigned Company, signed by way of acknowledgement and acceptance, and will be kept by said Company and made available to the Data Controller, if expressly so requested, no later than two days from the request itself;

- to avoid any unauthorized data processing, the undersigned Company will inform the Data controller of the termination of the employment relationship or the assignment in place no later than five days from the event, so that the Data Controller can arrange immediate revocation of the IT authorizations it issued.

Full name of the Sub-Processor's legal representative
Position
Name of the Sub- Processor
Date
Signature

Sub-processor of personal data

_____

By way of acknowledgement and acceptance - Authorized Person

_____

INSTRUCTIONS FOR "PERSONS AUTHORISED" TO PROCESS PERSONAL DATA

EU Regulation 2016/679 concerning the protection of personal data (hereinafter "GDPR") requires all those who process personal data to carry out operations with respect for and protection of the natural persons to which the data refer, whether they are employees, suppliers of goods and services, customers, consultants, etc..
The GDPR specifically envisages the need to provide adequate instructions for all those who, in relation to the implementation of their work, process personal data; in other words, those who use or become aware of personal data as described in Art.4 No. 1 of the GDPR (see definitions at the end).
In compliance with the provisions of the GDPR, as "Authorised Person" you shall process the relevant personal data by paying scrupulous attention to the following instructions and to all other instructions that may be provided by your Data Processor or the Data Controller or other person delegated by it.

Please remember that the personal data must be processed:

- in observance of the criteria of confidentiality;
- lawfully and correctly;
- for a period of time not exceeding that necessary for the purpose for which the data have been collected or subsequently processed;
- with total observance of suitable security measures, by storing and controlling the data subject of the processing in such a way as to avoid the risk, even accidental, of destruction or loss, of unauthorised access or processing that is not permitted or does comply with the purpose of the collection.

In particular, with regard to:

- **Access to personal data**, data banks and corporate applications: data, data banks and corporate applications you may access are those that are strictly indispensable for the implementation of your work, in line with your role and, as far as regards IT applications, in accordance with the user profile assigned to you.
- **Creation of new procedures/applications**: without prior authorisation, you cannot activate new IT procedures for the management or processing of data, files including hard copies, or personal data files. If the above is necessary, you must give your immediate superior prior notice and proceed only after receiving authorisation.
- **Communication and dissemination**: the data you have access to during your work must be processed by you personally, or by your colleagues, but cannot be communicated and/or transmitted to outside third parties.
- **Security measures**: it is your responsibility to observe all current protection and security measures aimed at preventing the risk of destruction, loss, unauthorised access or prohibited processing; in particular, your password must not be given to anyone, your PC must not remain connected to company files and accessible in your absence; hard copies of data must be placed in locked cabinets at the end of the day and always after being used; in any case, you must assure the confidentially of hard copies of data every time you leave your workstation. All episodes that you deem important as regards data security must be immediately communicated to your Manager. Special attention must be paid to the management of documents containing data of a juridical and/or sensitive nature.
- **Requests for access/exercise of rights**: if you receive a request to access personal data ex Chapter 3 "Rights of data subject" of the GDPR, from the data subject (whether it is an employee of the company, a supplier, a customer, a consultant, etc.), you must take note of the same in writing, specifying the date and the name of the data subject, and immediately refer the same to your Manager or to the relevant organisation office, which will respond within the established time frame.

1. PROCESSING WITHOUT ELECTRONIC DEVICES
Personal data filed on magnetic and/or optical media must be protected by the same security measures as those adopted for hard copies.
The security measures applied to copies or reproductions of documents containing personal data must be identical to those applied to the originals.

1.5 Safekeeping

Documents containing personal data must be stored in such a way that they are not accessible by persons not authorised to process them (e.g.: cabinets or drawers that can, if possible, be locked).
Documents containing personal data that are removed from the files for day-to-day work must be returned at the end of the day.
Documents containing personal data must not be left unattended on desks or work tables; similar attention must be paid when removing documents that have been received via fax; as a general rule you should avoid printing documents unless it is strictly necessary and in any case they must be removed immediately so that they are not left unattended at the printer.

1.6 Communications

The use of personal data must take place on the basis of the "need to know" principle and they must not be shared, communicated or sent to persons who do not require them for the implementation of their work (even if such persons are also authorised to process data). Data must not be disclosed outside the Company and in any case to third parties unless authorized by the Data Controller or the Data Processor.

1.7 Destruction

If it is necessary to destroy documents containing personal data, they must be destroyed by using the appropriate shredders or, in their absence, they must be cut into small pieces so that they cannot be reassembled.
Magnetic or optical media containing personal data must be erased before they can be reused. If this is not possible, they must be destroyed.

1.8 Additional instructions for processing sensitive and judicial data

Documents containing sensitive and/or judicial data must be controlled and stored by Authorised Persons in such a way that they cannot be accessed by unauthorised persons. For example, reference to documents/certificates for insertion in electronic personnel management/administration procedures, data regarding trade union authorisations, sick leave, etc., must take place in the time strictly necessary for keying in the same and, immediately after, the documents must be filed in accordance with these instructions. The filing of hard copies containing sensitive and/or judicial data must be kept separate from those concerning common data (the same cabinet or drawer may be used - and possibly locked - but the containers must be separate).
To access files containing sensitive or judicial data outside office hours you must be identified and recorded in the relevant registers.

2. PROCESSING WITH ELECTRONIC DEVICES

2.1 Management of authentication credentials

The law envisages that access to electronic procedures that process personal data is permitted by Authorised Persons in possession of "authentication credentials" which allow them to bypass an identification procedure. Authentication credentials consist of a code for identifying the Authorised Person for processing personal data (user-ID) associated with a confidential password, or an authentication device (e.g.: smart card, token, one-time-pw), or a biometric characteristic. Authorised Persons must use and manage their authentication credentials in accordance with the following instructions.
Individual user-IDs for accessing applications must never be shared amongst users (even if Authorised Persons for data processing). If other users must access data, they are required to request authorisation from their Manager.
Authentication credentials (for example passwords or strong authentication devices like tokens, smart cards, etc.) that allow access to applications must be kept confidential. They must never be shared with other users (even if Authorised Persons for data processing).
Passwords must be changed by the Authorised Person following the first use and subsequently, in observance of the specific corporate procedures, at least every three months in the case of sensitive and judicial data processing, or at least every six months for personal/shared data.
Passwords must consist of at least eight characters or, if this is not permitted by the electronic device, by the maximum number of characters permitted. Passwords must not contain references that easily lead to the Authorised Person (e.g.: family names) and must be chosen in accordance with corporate regulations concerning the construction and use of passwords (see also point 3, below), unless more restrictive instructions are envisaged by corporate systems.

2.2 Protection of PC and data

All PCs must have passwords that comply with the instructions given in the next point below. Passwords must be kept and managed with due diligence and in observance of the instructions provided by the Data Controller or, on its behalf, by the Data Processor.
To prevent illicit access, the screen saver password must always be activated if this setting is not automatically available.
As soon as they are available (and in any case at least annually) all software updates necessary for preventing vulnerability and correcting defects must be installed in the PCs. If this does not take place automatically, the Authorised Person must inform his/her Manager.
Back-up storage must be carried out at least every week on the assumption that any third party personal data are present only in the PC of the Authorised Person (not filed in corporate IT systems). The storage media used for back-up must be managed in accordance with the rules described in "Processing without electronic devices".

2.3 Deletion of personal data

In the event of disposal of work tools, it is your responsibility to eliminate all personal data they contain.

2.4 Additional instructions for processing sensitive and judicial data

Passwords for accessing IT procedures used to process sensitive and judicial data must changed, by the Authorised Person if an automated system is not available, at least every three months, unless more restrictive methods and time frames are communicated from time to time by the Manager or provided for in procedures.

The installation of software updates required to prevent vulnerability and correct computer program defects must be carried out at least every six months if an automated system is not available.

3. GENERAL INSTRUCTIONS

How to choose and use a password

- Use at least 8 characters
- Use letters, numbers and at least one character from . ; $! @ - > <
- Do not use your own or a relative's date of birth, name or surname
- Do not use a matriculation number or user ID
- Always keep it in a safe place that cannot be accessed by third parties
- Do not divulge it to third parties
- Do not share it with other users

Conduct in the presence of guests or service personnel

- Have guests wait in places where confidential information or personal data are not present.
- If necessary, move away from your desk when guests are present, put documents away and enable the PC screen saver by pressing “ctrl-alt-del” on the keyboard and selecting “Lock Computer”.
- Do not reveal passwords to technical assistance personnel and/or allow them to type in passwords.
- Do not reveal passwords over the telephone - no one is authorised to request them.

How to handle e-mails

- Do not open messages with attachments if you do not know the source since they could contain viruses that will delete or steal data stored in the PC.
- Avoid opening films, presentations, images and files in any format if they come from unknown sources since these could pose a threat to the data contained in your PC and, in general, to the security of the corporate technological infrastructure.
- Avoid forwarding automatically from your company mail box to external personal mail boxes and vice-versa.

How to use the Internet correctly

- Avoid downloading software from the Internet (utility programs, office automation, multimedia files, etc.) as these could pose a threat to the data and the company network, unless the software is required for the implementation of your work and its use is in any case known to the relevant corporate organisation offices.

4. PENALTIES FOR NON OBSERVANCE OF REGULATIONS

You are reminded that the use for personal purposes or in any case for unlawful aims of the data to which you have access or have accessed, even if it does not cause damage to and/or responsibility for the Controller, according to applicable Romanian law (Civil Code, Criminal Code etc.), could in any case be subject to the application of disciplinary or criminal penalties, as this could be construed as a breach of the duties that are incumbent on the employee, as envisaged by the Romanian Labour Code or by the applicable Collective or Individual Labour Agreement.

You are requested to promptly report any evidence of situations that put the security of data at risk (e.g.: password breach, attempted unauthorised access to the systems) or which concern external subjects authorised to access (obvious breach of corporate Procedures): your collaboration is important for closing any gaps in the security systems and procedures for protecting the personal data processed.

These instructions are the guidelines to be followed for your work: inasmuch, if in doubt, please contact the Manager.

5. DEFINITIONS

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.

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, cultural or social identity of that natural person;

Special categories of data: personal data that reveal racial or ethnic origins, political opinions, religious or philosophical beliefs or trade union membership, as well as biometric data intended to unequivocally identify a natural person, data concerning the health or sexual history or orientation of the natural person (Ed: disabilities, medical certificate, indication of illnesses/accidents, handicaps, etc.).

Judicial data: personal data that will reveal criminal convictions and offenses or to other related security measures with regard to criminal records, the register of crime-related administrative penalties and the relevant pending charges, or the status of the accused or suspect pursuant Romanian Code of Criminal Procedure and Criminal Code (e.g.: imprisonment or house arrest, legal disqualification, provisions relating to amnesty and pardon, etc.).

Data controller: the 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;

Processor: the natural or legal person, public authority, agency or other body which processes personal data on behalf of the Data Controller;

Authorized Person for data processing: Person authorized to process personal data under the direct authority of the Data Controller or the Data Processor.

Data subject: the natural person to whom the personal data refer (e.g.: employees, customers, suppliers, visitors, etc.).

Security measures: All the technical and organisational measures that adequately guarantee a level of security adequate to the risk (Ed: pseudonymisation, encryption, user id, password, use of containers with locks, etc.).

Personal data breach: means 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.

Attachment GDPR 8

Appointment as Authorized Person for Processing Personal Data (hereafter "Authorized Person"), pursuant to Article 29 of EU Regulation 2016/679 (hereafter "GDPR ") by the Sub-Processor
SUBSTITUTIVE DECLARATION

Messrs
[•]

The undersigned .....
(surname) (name)……..
born in ..... (.....), on ……..……
(place) ..... (prov.) ....
resident in …….. (…….) Address …… n. …
(place)…….. (province.)…… (address)……
domiciled in ..... (.....) in Address ..... n. ...
(place)…….. (province)…… (address)……
as legal representative of the Firm / Company .....
with registered head offices in ..... (.....) Address ..... n. ...
Tax Code ……..VAT n. ……..

with reference to Contract n. .....

as Sub- Processor, aware of the penal sanctions referred to in the Romanian Criminal Code – chapter VI - as regards false declarations and the creation or use of false documents, under his/her own responsibility

DECLARES

- having appointed employees/collaborators in relation to the activities referred to in the above-mentioned contract as **"Authorized Persons"** for processing personal data as per Article 29 of the GDPR using the template appointment letter prepared by you including the related Instructions
- that a copy of these appointments in his/her possession is available and at the disposition of this company

HEREBY ATTACHES

- to this document the list of names of persons appointed for this purpose

UNDERTAKES

- to provide the Company with a copy of appointed persons by the date that will be specifically notified by the Company;
- to update the documentation sent, before starting activities in the case of new employees/collaborators or within five working days from the date of termination when employees/collaborators are no longer involved.

Full name of the legal representative
Position
Name of the Company
Date
Signature

Privacy notice pursuant to Article 13 of the GDPR

We hereby inform you that personal data are acquired with this Annex and are processed for purposes strictly related to the management and execution of the Contract or to implement obligations required by law. Additionally, personal data will be collected and processed using automated means and in paper form and will be stored for the entire duration of the Contract and after its termination for a period not exceeding the terms envisaged by applicable laws.

In this respect, it should be noted that:

– the Data Controller for the data in question is the following Enel Company [•] in the person of its pro tempore legal representative (hereafter "Controller");

- The data subject is the natural person whose personal data are processed for the purposes of stipulation, management and execution of the Contract (hereinafter the data subject);
- The personal data processed may be transmitted to third parties, i.e. to companies subject to management and coordination by ENEL S.p.A. or connected with ENEL, or to other subjects. The above-mentioned third parties may be appointed as Data Processors
- The data subject is entitled to exercise the rights envisaged in Articles 15-21 of the GDPR (right to access data, request their rectification, portability or cancellation, request the limitation of processing of data concerning him/her or may oppose processing), where applicable, by contacting the Data Controller;
- The data subject is entitled to lodge a complaint to theRomanian Data Protection Authority (ANSPDCP), with registered office in Bucuresti, B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, cod postal 010336, Romania, Tel. (+40) 318059211 or (+40) 318059212, email: anspdcp@dataprotection.ro;;
- The Data Controller has appointed the Data Protection Officer (DPO) pursuant to Article 37 of the GDPR, whose contact details can be found on the Data Controller's website.

N.B. The signature of the owner or legal representative must be accompanied by non-authenticated photocopy of the signer's identity document (front/rear)

Attachment GDPR 9

Notification regarding the breach of security of personal data processing

To: .....
In the attention of: .....
Regarding: .....
Date: .....

Whereas:

- The agreement concluded between Enel …., a Romanian legal entity with registered office in …..., J……, Tax Identification Number……., duly represented by …… as …. (Hereinafter referred to as "Beneficiary" or "Controller") and ……, a Romanian legal entity with registered office in ……, J……., Tax Identification Number ……..., represented by ……..…. as …..... (Hereinafter referred to as "Supplier" or "Processor"), for the period ……..…….. - ……..., having as subject-matter ……. , and a duration of ....., respectively from ..... until ....., (hereinafter referred to as "Contract");
- Capacity as processor of …….. within the meaning of the provisions of Regulation no. 679/2016 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 (hereinafter referred to as "GDPR") and the Romanian Law no. 190/2018 related to GDPR implementation;

1. We hereby inform you that on ……, at ……..., the Processor took note of the appearance/existence of a security breach in the system/application/server/database ……, managed/administered by:

- ☐ Employees of the processor [3];
- ☐ The contractual partners of the processor [4];
- ☐ Sub-processors [5].

Date and time (h/min/sec) of the data breach incident: ……

Date and time (h/min/sec) of the data breach incident acknowledgment: ……..

Brief of the data breach incident: ……
……..……
……
……..

Type of the servers and their location: …….. ……
……..……
……
……..

2. The processor took note of the appearance/existence of the above-mentioned security breach as a result of:

- ☐ Receiving an information from……..
- ☐ Carrying out the ordinary monitoring/checking/auditing activities;
- ☐ Carrying out the specific monitoring/checking/inspection/auditing activities;
- ☐ Others (*please specify*): .....
.....;

Art. 3. Furthermore, we hereby mention as follows:

[3] Its own employees (any person involved in employment contractual relations with the processor; for the purposes hereof, the parties detached within ENEL Group's companies in Romania are also assimilated to the employees, as well as the persons carrying out their activity within ENEL, pursuant to a staff leasing agreement, the directors or managers, as defined under the Law no. 31/1990 on companies).
[4] All contractual partners, their employees, the external auditors, consultants, subcontractors/ authorized natural persons, legal representatives, collaborators/third party contractors/ sub-contractors/partners or third party supporters participating in the public procurement procedures/ legal entities or authorized natural persons who provide services, supply goods and/or perform works.
[5]The natural person or legal entity, public authority, agency or other body processing the data upon the request of the Processor. Any such data processing operations are only possible subject to compliance of the provisions of the Controller mentioned herein.

a) the description of the nature of the breach of security of the personal data: ……..
……
……
……
……
……

b) the approximate number of data subjects shall be of ……, these being part of the category:
- ☐ Controller's Employees[6];
- ☐ Controller's clients;
- ☐ Collaborators[7] of the Controller;
- ☐ Others (*please specify*): .....
.....;

c) the categories of the personal data affected: ……., mainly
……
……

d) number of data subject affected: ……

e) the possible negative consequences of the breach of security of the personal data are: ……
……
……
……

f) the actions already taken by the Processor in order to remedy the issue regarding the breach of security of the personal data, including, as the case may be, the measures to mitigate its possible effects are:
……
……
……

g) other actions proposed to be taken by the Processor in order to remedy the issue regarding the breach of security of the personal data, including, as the case may be, the measures to mitigate its possible effects are:
……
……
……
……

- ☐ The costs for the implementation of these measures are included in the price of the Contract, the execution duration thereof being of approximately …….. calendar days;
- ☐ The costs for the implementation of these measures are NOT included in the price of the Contract; the total maximum estimated costs amount to Euro …… and represent approximately ……% of the total amount of the Contract, their execution duration being of approximately …….. calendar days;
- ☐ Not applicable.

4. The Processor, as professional for the purpose of art. 3 of the Romanian Civil Code as well as in consideration of the obligations incumbent upon it by virtue of the Regulation, considers that:

The breach of security of personal data processing and taking into account the provisions of WP 29 opinions [8],
- ☐ The above-mentioned security incident is liable to generate a high risk for the rights and freedoms of the data subject, as
……
……
……
- ☐ The above-mentioned security incident is NOT liable to generate a high risk for the rights and freedoms of the data subject, as
……
……

[6] Persons involved in employment contractual relations with ENEL; for the purposes hereof, the persons attending traineeships, the persons detached within ENEL Group's companies in Romania are also assimilated to the employees, as well as the persons carrying out their activity within ENEL, according to a staff leasing agreement, the internal auditors, directors or managers, as defined by the Companies Law no. 31/1990.

[7] The counterparties of ENEL, their employees, the external auditors, consultants, subcontractors/ authorized natural persons, legal representatives, collaborators/third party contractors/ sub-contractors/partners or third party supporters participating in the public procurement procedures/ legal entities or authorized natural persons who provide services, supply goods and/or perform works.

[8] WP 248 – Impact Assessment Guide on the data protection (DPIA) and the determination whether a processing operation is liable to generate a high risk within the meaning of the Regulation and wp 250 – Guide regarding the notification of the security incidents within the meaning of the Regulation.

……
The above-mentioned security incident is of the type: ☐ Incidents which concern the confidentiality: when there is unauthorized or accidental disclosure of personal data; ☐ Incidents which concern the availability: when there is unauthorized or accidental destruction/erasure of personal data; ☐ Incidents which concern the integrity: when there is unauthorized or accidental variation of personal data;

5. Moreover, we mention that the above-described security incident was included in the Register of personal data processing operations carried out by the Processor.

6. The Processor shall not be held responsible for the issue of the opinion within art. 4 above, as the opinion of the Processor shall have a strictly advisory role.

7. Does the data breach affects data subjects from other UE member states?

☐ No
☐ Yes. Please describe: ……..
……..
……..

8. The notification of another competent data protection authority is needed?

☐ No
☐ Yes. Please describe: ……..
……..
……..

9. For more additional information regarding this incident please contact Mr./Mrs.
……– specialist in
……., mobile ……,
email address ……., as responsible for dealing with the above-mentioned security incident.

Full name of the Processor's legal representative
Position
Name of the Processor
Date
Signature