This "ANNEX VII Italy" applies to the supply, services and works contracts governed by the Italian law and established between a company of the ENEL group and a Contractor.

CONTENTS

SECTION I - GENERAL PART.

1. GENERAL INFORMATION.

1.1. This “ANNEX VII Italy” applies to the supply, services and works contracts (hereinafter also referred to as "Contract") governed by the Italian law and established between a company of the ENEL group and a Contractor (jointly referred to as the "Parties").

1.2. This document forms an integral and substantial part of the General Terms and Conditions of Contract of the Basic ENEL group (hereinafter referred to as “General Terms”) to which it is annexed. The web page on which the General Terms – General Part and this Annex VII Italy are provided is indicated in the Order Letter and, upon request, a copy in digital/paper format will be sent to those who do not have access to said web page.

1.3. Without prejudice to the terms set forth in Article 1 “GENERAL INFORMATION” of the General Terms – General Part, any derogation to or amendment of this Annex VII Italy proposed by the Contractor will only be valid if made in writing and accepted in the same form by ENEL. It will only be applicable to the Contract for which it has been proposed, with no possibility that the exception can be extended to other ongoing contracts or any contracts that might be established subsequently with the above-mentioned Contractor.

1.4. In case of any discrepancies or incompatibility between the documents that form part of the Contract, reference shall be made to Article 1. “GENERAL INFORMATION” of the General Terms – General Part in which the parties establish that prevalence will be assigned to the progressive order in which the contract documents are listed therein.

1.5. The original version of this Annex VII Italy is the Italian version. In case of a discrepancy between the original version in Italian and the translations in other languages, the original version in Italian will prevail.

1.6 Unless otherwise established within the Contract, the legislation applicable to the Contract is the Italian law and the competent jurisdiction for any litigation that may arise between the Parties regarding the interpretation or execution of the above-mentioned Contract is the Court of Rome.

2. CONTRACTOR'S DUTIES

2.1. The Contractor undertakes, for the entire duration of the Contract, to perform the service which is the subject of the Contract in line with the conditions, methods, terms and provisions contained in the documents which form part of the Contract. They also guarantee to ENEL that all the activities will be carried out with due professional diligence, using the best techniques available, according to the highest standards of workmanship and by qualified personnel who are qualified to perform them.

3. CONTRACT PRICES

3.1. General information.

3.1.1. Without prejudice to the terms set forth in Article 3 “ECONOMIC TERMS AND CONDITIONS”. and Article 3.1. “PRICE” of the General Terms – General Part, unless otherwise established within the Contract, the contract prices, in derogation to Article 1664 of the Italian Civil Code, shall be fixed and invariable for the entire duration of the Contract.

3.1.2. When signing the Contract, the Contractor acknowledges:

- that they have been fully informed regarding the type of services that are the subject of the above-mentioned Contract, the type of places, local conditions and all other elements necessary and that they have assigned due consideration to these in relation to all the circumstances and hazards that might affect the execution of the services and how the relative prices are determined;
- that, for the elements described above, no reservations can be raised regarding the poor profit margin of the individual prices, regardless of the reasons that may have determined this.

3.1.3. Should the Contractor, on their own initiative and without the written approval of ENEL, perform services/works/jobs/interventions of a higher quantity and quality than those commissioned, or use material and equipment that are bigger or of a superior quality than those established, they will not be entitled to receive higher payments, but only payment of the amounts due for the elements as commissioned.

3.2. Price Review;

3.2.1. The contract prices can only be reviewed if this is envisaged in the Contract and if the duration of the Contract is longer than a year from the initial date agreed upon between the Parties, or from another date referring to the beginning of the activities indicated in the Contract, including any suspensions of the same that may be ordered by ENEL and excluding any causes for delay ascribable to the Contractor.

3.2.2. The price review is requested by the interested party and calculated using the methods indicated in the Contract; if calculated by the Contractor, ENEL reserves the right to cross-check the calculation.

3.2.3. The amounts paid to the Contractor specified in the accounting documents which refer to the services performed after the expiry of the first year from the initial date agreed upon by the Parties, or from another date which refers to the commencement of the activities indicated in the Contract, can be subject to review.

3.2.4. For both Parties, the agreement reached with reference to the price review constitutes full acknowledgement of all the respective rights and duties, also in relation to any variations – that is, increases or reductions – in the costs.

3.2.5. The amount of the price review does not affect the composition or calculation of the amount of the Contract.

4. INVOICING AND PAYMENTS

4.1. General information.

4.1.1. Without prejudice to the terms set forth in the General Terms - General Part, Article 3 “ECONOMIC TERMS AND CONDITIONS” and Article 3.3 “INVOICING”, with the exception of Letter “B” of point 3.3.2 of the above-mentioned Article, the amounts due must be invoiced by the Contractor pursuant to the methods and terms established in the Contract.

In particular, in derogation to the terms set forth in point 3.3.2 Letter “B” of Article 3.3 “INVOICING”, the invoices must only be sent using the electronic systems of ENEL (Procurement Portal).). Suppliers that are resident in Italy and any that are not resident but operate in Italy through a permanent establishment or another type of establishment that identifies them for the purposes of applying VAT, must send their invoices using a structured digital format (xml).

Non-resident suppliers can only send the invoice in TIFF/PDF format, using the designated channel active in the WEB EDI Portal.

Even if the Contract establishes that invoices can be paid with different currencies, each individual invoice must be issued in a single currency.

4.1.2. The invoice will only be valid and ENEL can only accept it if it contains all the data envisaged in the Contract and by the applicable law, and if the activity that forms the subject of the Contract has been correctly executed. The invoices must contain all the information required by the tax legislation in force.

4.1.3. Except in case the Temporary Consortium or ordinary Consortium has an autonomous VAT number, each member company must invoice the amounts due for their own service, also in order to comply with the duties of financial traceability set forth in Article 5 below “TRACEABILITY OF THE FINANCIAL FLOWS”. The invoices issued by the individual companies must be received by ENEL suitably accompanied by the approval of the representative company.

4.1.4. Without prejudice to the legislation in force regarding public contracts, the Parties in any case understand that, in case of subcontract or piecework, where ENEL has not declared that it will pay the subcontractor or piece worker the amount due for the services performed by the same directly, ENEL will suspend the payment to the Contractor, if the Contractor has failed to send, a copy of the invoices settled by the Contractor's payments to the subcontractor or piece worker, indicating the amounts withheld for the purposes of guarantee, by the deadlines established by the law.

4.1.5. ENEL in any case reserves the right not to make payments if the Contractor fails to: comply fully with the duties specified in this Contract; have met all the requirements for compliance defined by Law; in particular with the competent Authorities, the labour force employed and third-parties in general; comply with the terms set forth in Article 5 below "TRACEABILITY OF THE FINANCIAL FLOWS".

4.1.6. The Contractor cannot appoint third parties to receive payments or issue any form of payment delegation.

4.2. Payments.

A) <u>The clauses in points 4.2.1. and 4.2.2., are applicable to the contracts for activities assigned pursuant to the law in force regarding public contracts (so-called Procurement Code).</u>

4.2.1. Contract for services and/or works (pursuant to the law in force regarding public contracts).

4.2.1.1. Before issuing each invoice, the Contractor must request the approval of the ENEL Unit that manages the Contract. Such approval shall be issued subject to ENEL carrying out any checks that may be required by law or by the contract for the purpose of ascertaining the conformity of the services with the provisions of the contract.

4.2.1.2. The invoices will be paid by bank transfer with a fixed value date for the beneficiary, on the third last working day of the month in which the deadline of 60 days from the end of the month in which the invoices are received falls, as long as the invoices reach ENEL complete with the details of the authorisation to issue payment (payment approval). Should the payment approval - which can be found using the functions present on the Portal - be missing, instead the invoices must always specify:

- the purchase order number;
- the name of the Unit at which the service was rendered or the supply provided

If the details of the authorisation to invoice are not specified on the invoices, these will not be accepted or considered for the purposes of calculating the date of receipt.

4.2.1.3. Should the payment date, as defined above, fall on a Monday or Tuesday, the payment will be postponed until the following Wednesday, if this falls on a working day; otherwise the payment date will remain the same.

4.2.1.4. In case of a delay in payment that exceeds the term established within the contract, where said delay is ascribable to ENEL, the Contractor will be owed interest in the measure of the legal interest calculated as indicated below:

1. For the first half of the year to which the delay refers, the legal interest in force on 1 January of that year will be applicable;

2. For the second half of the year to which the delay refers, the legal interest in force on 1 July of that year will be applicable.

For the application of the rates as described in points 1 and 2 above, reference will be made to the rate published in the Official Journal of the Italian Republic by the Ministry of Economy and Finance, on the fifth working day of each calendar six-month period.

Interest will be applicable, with no need for issuance of a formal notice of default, from the day following the payment term established in the Contract.

4.2.1.5. Should the creditor prove that they have sustained costs for recovering the credit, the same will be entitled to receive a lump sum of Euro 40 (forty/00 euro) as damage compensation,with no need for issuance of a formal notice of default. The above is true without prejudice to the parties' right to prove that further damages have been suffered, which can include the costs sustained for recovering the credit.

4.2.2. Supply contract[1] (pursuant to the law in force regarding public contracts).

4.2.2.1 The invoices will be paid by bank transfer with a fixed value date for the beneficiary, on the third last working day of the month in which the deadline of 60 days from the date of acceptance by ENEL falls, or the date of any checks that ENEL may be required to perform by law or by the Contract in order to ascertain the conformity of the goods to the terms set forth in the Contract (approval date). This is true subject to the invoices reaching ENEL complete with the details of the authorisation to issue payment (payment approval). Should the payment approval - which can be found using the functions present on the Portal - be missing, instead the invoices must always specify:

- the purchase order number;
- the name of the Unit at which the service was rendered or the supply provided.

If the details of the authorisation to invoice are not specified on the invoices, these will not be accepted or considered for the purposes of calculating the date of receipt.

4.2.2.2 Should the payment date, as defined above, fall on a Monday or Tuesday, the payment will be postponed until the following Wednesday, if this falls on a working day; otherwise the payment date will remain the same.

4.2.2.3. In case of a delay in payment that exceeds the term established within the contract, where said delay is ascribable to ENEL, the Contractor will be owed interest in the measure of the legal interest calculated as indicated below:

1. For the first half of the year to which the delay refers, the legal interest in force on 1 January of that year will be applicable;

2. For the second half of the year to which the delay refers, the legal interest in force on 1 July of that year will be applicable.

For the application of the rates as described in points 1 and 2 above, reference will be made to the rate published in the Official Journal of the Italian Republic by the Ministry of Economy and Finance, on the fifth working day of each calendar six-month period.

Interest will be applicable, with no need for issuance of a formal notice of default, from the day following the payment term established in the Contract.

4.2.2.4. Should the creditor prove that they have sustained costs for recovering the credit, the same will be entitled to receive a lump sum of Euro 40 (forty/00 euro) as damage compensation,with no need for issuance of a formal notice of default. The above is true without prejudice to the parties' right to prove that further damages have been suffered, which can include the costs sustained for recovering the credit.

B) <u>The clauses in points 4.2.3. and 4.2.4., are applicable to contracts regarding activities assigned NOT pursuant to the law in force regarding public contracts (so-called Procurement Code).</u>

4.2.3. Contract for services and/or works (not pursuant to the law in force regarding public contracts).

4.2.3.1. Before issuing each invoice, the Contractor must request the relative approval of the ENEL Unit that manages the Contract. Such approval shall be issued subject to ENEL carrying out any checks that may be required by law or by the contract for the purpose of ascertaining the conformity of the services with the provisions of the contract.

The invoices will be paid by bank transfer with a fixed value date for the beneficiary, on the third last working day of the month in which the deadline of 60 days from the end of the month in which the invoices are received falls, as long as the invoices reach ENEL complete with the details of the authorisation to issue payment (payment approval). Should the payment approval - which can be found using the functions present on the Portal - be missing, instead the invoices must always specify:

- the purchase order number;
- the name of the Unit at which the service was rendered or the supply provided.

If the details of the authorisation to invoice are not specified on the invoices, these will not be accepted or considered for the purposes of calculating the date of receipt.

4.2.3.3. Should the payment date, as defined above, fall on a Monday or Tuesday, the payment will be postponed until the following Wednesday, if this falls on a working day; otherwise the payment date will remain the same.

[1] In supply contracts and supply and installation contracts that envisage invoicing plans and which envisage that the goods that form the subject of the Contract are only delivered once ENEL has authorised said delivery, the clause relative to service contracts will be applied.

4.2.3.4. In case of a delay in payment that exceeds the term established within the contract, where said delay is ascribable to ENEL, the Contractor will be owed interest in the measure of the legal interest calculated as indicated below:

1. For the first half of the year to which the delay refers, the legal interest in force on 1 January of that year will be applicable;
2. For the second half of the year to which the delay refers, the legal interest in force on 1 July of that year will be applicable.

For the application of the rates as described in points 1 and 2 above, reference will be made to the rate published in the Official Journal of the Italian Republic by the Ministry of Economy and Finance, on the fifth working day of each calendar six-month period.

Interest will be applicable, with no need for issuance of a formal notice of default, from the day following the payment term established in the Contract.

4.2.3.5. Should the creditor prove that they have sustained costs for recovering the credit, the same will be entitled to receive a lump sum of Euro 40 (forty/00 euro) as damage compensation,with no need for issuance of a formal notice of default. The above is true without prejudice to the parties' right to prove that further damages have been suffered, which can include the costs sustained for recovering the credit.

4.2.4. Supply contract[1] (not pursuant to the law in force regarding public contracts).

4.2.4.1. The invoices will be paid by bank transfer with a fixed value date for the beneficiary, on the third last working day of the month in which the deadline of 60 days from the date of acceptance by ENEL falls, or the date on which any checks that ENEL may be required by law or by the Contract to perform to ascertain the conformity of the goods are executed (approval date). This is true subject to the invoices reaching ENEL complete with the details of the authorisation to issue payment (payment approval). Should the payment approval, which can be found using the functions present on the Portal, be missing, the invoices must always instead contain:

- the number of purchase order;
- the indication of the Unit at which the service was rendered or the supply provided

4.2.4.2. Should the payment date, as defined above, fall on a Monday or Tuesday, the payment will be postponed until the following Wednesday, if this is a working day; otherwise the payment date will remain the same.

4.2.4.3. In case of payment delay that exceeds the term of the contract, where said delay is ascribable to ENEL, the Contractor will be owed interest in the measure of the legal interest calculated as indicated below:

1. For the first half of the year to which the delay refers, the legal interest in force on 1 January of that year will be applicable;
2. For the second half of the year to which the delay refers, the legal interest in force on 1 July of that year will be applicable.

For the application of the rates as described in points 1 and 2 above, reference will be made to the rate published in the Official Journal of the Italian Republic, by the Economy and Finance, on the fifth working day of each calendar six-month period.

The interest will be applicable, with no need for issuance of a formal notice of default, from the day following the payment terms established in the Contract.

4.2.4.4. Should the creditor prove that they have sustained costs for recovering the credit, the same will be entitled, with no need for issuance of a formal notice of default, to a lump sum of Euro 40 (forty/00 euro) as damage compensation. The above is true without prejudice to the parties right to prove that further damages have been suffered, which can include the costs sustained for recovering the credit.

5. TRACEABILITY OF THE FINANCIAL FLOWS[2].

5.1. The Contractor undertakes all the duties as specified in Article 3, of Law no. 136 of 13 August 2010, (Traceability of financial flows), as amended by Italian Decree Law no. 187 of 12 November 2010, converted with Law no. 217 of 17 December 2010.

5.2. In particular, to ensure the traceability of the financial flows in order to prevent criminal infiltrations, the contractors, subcontractor and subcontracting parties of the chain of companies and the parties that provide public funding, including European funding, for any reason in relation to the public works, services and supplies, must use one or more bank or post office accounts, opened at banks or at the company Poste Italiane Spa, dedicated to the Contract, also not on an exclusive basis, without prejudice to the terms set forth in paragraph 5 of above-mentioned Article 3.

5.3. Additionally, all the financial transactions relative to the public works, services and supplies and, therefore to the Contract, as well as to the management of the above-mentioned funding, must be registered in the dedicated current accounts and, without prejudice to the terms of paragraph 3 of above-mentioned Article 3, they must only be performed by way of bank or post office transfer or using other tools for receiving or making payments that appropriately ensure the full traceability of the operations.

5.4. The Contractor must communicate to the competent Administrative Departments of ENEL, the details identifying the dedicated current account described above within seven days from when it is opened or, in the case of existing current accounts, from the

[2] The clause is only applicable to the contracts assigned pursuant to the legislation in force regarding public contracts.

first time they are used in financial operations related to the Contract, and, by the same deadline, the general details and tax codes of the persons delegated to operate on the same.

Similarly, and by way of the same methods, the subcontractor or the subcontracting party via the Contractor, must communicate the data described above to the Contract Manager.

5.5. The Contractor, the subcontractor or the subcontracting party who learns of its counterpart's non-fulfilment of the duties to ensure financial traceability, must inform ENEL and the local government Prefecture Office competent for that area accordingly.

5.6. The Contractor also undertakes to add into the contracts with its subcontractors or sub-contracting parties a similar clause by which each one undertakes all the duties to ensure the traceability of the financial flows as set forth in the above-mentioned Article 3, of Law no. 136 of 13 August 2010.

5.7. Should the Contractor breach even only one of the duties set forth in Article 3 of Law no. 136 of 13 August 2010, or in this Article, the Contract will automatically be terminated immediately, pursuant to and by virtue of Article 1456 of the Italian Civil Code.

5.8. Should, in addition to the Tender Identification Number (CIG), the mandatory issuance of the Single project Code (CUP) also be required, ENEL will communicate said code to the Contractor who will state the same on each relative transaction.

6. "ANTIMAFIA" LEGISLATION, PROTOCOLS OF LEGALITY, SUBCONTRACT, CREDIT AND CONTRACT TRANSFERABILITY.

6.1. General information.

6.1.1. The Contract must be executed in compliance with all the duties envisaged by the antimafia law and by the Protocols of legality in force established by ENEL. The Contractor states that they have viewed and accept the terms stated in the above-mentioned protocols and that they undertake to comply with and implement the same.

These same terms must be included in any subcontracting contracts established by the Contractor.

6.2. Subcontracting and Subcontracts.

6.2.1. Subcontracting is permitted within the limits defined by the applicable legislation and/or the terms set forth in the Contract, subject to a check on the part of ENEL.

For contracts subject to the **law on public contracts,**

the Contractor will be responsible for forwarding the request to establish a subcontract, providing, for each subcontractor:

1. A declaration certifying that they did not participate in the procedure for assigning the contract;
2. Proof of possession of the required qualification;
3. Specific self-certification (e.g. so-called ESPD), certifying the absence of any grounds for exclusion of the interested party as set forth by the legislation in force regarding public contracts;
4. Certificate of labour compliance (DURC);
5. Self-declaration certifying the interested party's compliance with the occupational health and safety obligations in relation to its employees;
6. Declaration issued by the subcontractor pursuant to Article 47 of Presidential Decree 445/2000 certifying that the interested party has an adequate labour force with the specific professional skills necessary to safely perform the subcontracted activities; that they have participated in training activities on the risks of the subcontractor company regarding the execution of the activities that form the subject of the subcontract; or that they undertake to provide said training activities for their workers particularly with reference to the specific risks in the environment in which they are destined to work and any risks caused by interferences before the commencement of the subcontracted activities;
7. All other documentation requested in the Order Letter.

Once authorisation has been obtained, the Contractor must register the copy of the subcontracting agreement signed by the parties at least 20 days before the effective commencement of the subcontracted activities.

For the contracts **not subject to the**legislation in force regarding public contracts, the Contractor will be responsible for forwarding the request to subcontract the work, providing for each subcontractor:

1. Proof of possession of the required qualification;
2. Specific self-certification (e.g. so-called ESPD), certifying the absence of any grounds for exclusion of the interested party as set forth by the legislation in force regarding public contracts;
3. certificate of labour compliance (DURC);

4. Self-declaration certifying the interested party's compliance with the occupational health and safety obligations in relation to its employees;

5. Declaration issued by the subcontractor pursuant to Article 47 of Presidential Decree 445/2000 certifying that the interested party has an adequate labour force with the specific professional skills necessary to safely perform the subcontracted activities; that they have participated in training activities on the risks of the subcontractor company regarding the execution of the activities that form the subject of the subcontract; or that they undertake to provide said training activities for their workers particularly with reference to the specific risks in the environment in which they are destined to work and any risks caused by interferences before the commencement of the subcontracted activities;

6. All other documentation requested in the Order Letter.

Once authorisation has been obtained, the Contractor must register the copy of the subcontracting agreement signed by the parties at least 20 days before the effective commencement of the subcontracted activities.

6.2.2. Without prejudice to the terms established above in Article 4 “INVOICING AND PAYMENTS”, point 4.1.4., the Contractor authorised to subcontract the activities must pay the subcontractor the amount due for the activities performed by the latter, send a copy of the invoices settled by the payments made to the subcontractor paid to the ENEL Department that manages the Contract, within 20 days from the date on which each payment is made.

6.2.3, If the Contractor fails to send the invoices and documentation described above by the above-mentioned term, ENEL will suspend payment of the amounts due based on the accounting progress reports, until the non-fulfilment has been fulfilled. This will not entitle the Contractor to claim any indemnity or damage compensation from ENEL nor will any interest accrue on the amount due.

6.2.4. The Contractor is jointly liable, with the subcontractor, for fulfilling this requirement, with both parties accepting responsibility for the safety duties envisaged by the legislation in force.

6.2.5. Should ENEL, during the execution of the subcontracted activities, find that a subcontractor fails to meet or no longer meets one of the conditions envisaged by the applicable legislation in force and/or by the Contract, it can proceed, depending on the case, in withdrawing the authorisation or in suspending the relative activities until the cause of the relative suspension ceases to exist. In the latter case, ENEL will warn the Contractor to ensure that the identified irregularities are eliminated within the term of 30 days from receipt of the warning, otherwise the authorisation of the subcontracting agreement will be withdrawn.

The Contractor must arrange to replace any subcontractors for whom this check identifies grounds for exclusion as set forth in the legislation in force on public contracts.

6.2.6. Following withdrawal of the authorisation, the Contractor must immediately terminate the subcontracting Contract and undertake to perform the relative activities itself, with no additional obligation for ENEL and without prejudice to the right to claim for any damages suffered by ENEL.

6.2.7. All contracts with subcontractors and Contractors must contain all the provisions contained in the Contract, including the specific indication of the safety costs, which must be paid in full and cannot be reduced .

6.2.8. Non-fulfilment of the above-mentioned envisaged duties – including those ascribable to the subcontractor – will constitute grounds for the termination of the Contract, pursuant to and by effect of Article 1456 of the Italian Civil Code.

6.2.9. The Contractor must communicate the name of the subcontractor, the amount of the Contract and the activities assigned to the ENEL Department that manages the Contract, for all the subcontracts established in relation to the execution of the contract.

6.3. Transfer of rights and credits.

6.3.1. The credits generated by the Contract can only be transferred to the Banks and Financial Intermediaries registered in the specific Rolls as set forth by Italian Legislative Decree no. 385 of 1 September 1993.

6.3.2 . ENEL must be notified that any credits generated by the Contract have been transferred only by sending a digital signature certificate sent by certified public email to the address of the interested ENEL company, indicated in the Contract, not later that 30 days prior to the term for the payment of the invoice relative to the transferred credit.

6.3.3 Pursuant to this Contract, the term "transfer of credits" is defined as the transfer of all the credits generated by the Contract to a sole transferee. Should the supplier intend to transfer the individual credits generated by this Contract to several transferees, they must notify ENEL accordingly in advance by public certified email, without prejudice to the duties described in Article 6.3.2.

6.3.4 .The details of the bank account(s) (from which the payments will be made) must always be those of the transferee. The transfer will be notified by the transferor or the transferee (by way of the methods envisaged in point 6.3.2); if notice is served by the transferee, it must be accompanied by an attachment; this attachment must be the deed of transfer stating the acceptance of the undersigned transferor by way of a certified digital signature.

6.3.5. The Parties understand that ENEL reserves the right not to proceed in paying the transferred invoice should the transferee prove not to hold the requisites described in point 6.3.1. of this article and should they not have formalised the communication in line with the methods envisaged in the previous points.

The above is true without prejudice to the right of ENEL, in its capacity as transferred obliger, to raise against the transferee all the exceptions that it would have been entitled to raise against the transferor.

6.3.6 The Contractor is forbidden from transferring the Contract or even only a part of the same.

7. DUTIES, TAXES AND FISCAL REPRESENTATION, NON-EU COUNTRIES.

7.1. The Contractor shall be liable for all registration duties and stamp duty as well as all the other rights and other taxes payable in relation to the elements that form the subject of the Contract.

7.2. The Contractor shall also be liable for the relative customs and tax operations. To this end, Contractors whose registered office is not located in one of the member states of the European Community must elect, for the purposes of performing the customs and tax operations, a fiscal representative resident in Italy which will be subject to the provisions of Presidential Decree no. 633 of 26 October 1972 as amended.

7.3. The appointment of the fiscal representative must be formalised by issuing a public deed or a notarised private agreement or, alternatively a letter registered in the specific register at the competent VAT Office or Inland Revenue Agency, and it must be communicated to ENEL within a month from the date on which the Contract is established and, in any case, at least 1 month before the beginning of the deliveries, and it must be valid for the entire duration of these deliveries. The details which identify the fiscal representative, once one is appointed, must be indicated in the invoice.

8. "SPLIT PAYMENT".

8.1. The current terms of Article 17-ter of Presidential Decree no. 633/1972 as amended by Legislative Decree no. 50/2017, provide for the application of the split payment method – for the period 1.7.2017 – 30.06.2020, without prejudice to future extensions - also to transfers of assets and provisions of services to the subsidiaries, in law or in fact, directly by the Chairmanship of the Council of Ministers or Ministries, and to any companies legally owned, either directly or indirectly by the same. To identify the above-mentioned parties, reference must be made to the lists regularly developed by the Department of Finance of the Ministry of Economy and Finance, published on the relative institutional website. When the invoices for the transfers /services received by the ENEL client company are issued, should said company be included in the above-mentioned lists with current validity (pursuant to Article 5-ter of the Decree of the Ministry of the Economy and Finance of 23 January 2015 as amended by the Decree of the Ministry of the Economy and Finance of 27 June 2017), the split payment regime will be applied to the invoices, unless these - by way of express provisions made in the legislation or in line with common procedure - are excluded from the above-mentioned regime (e.g. operations in reverse charge).

9. WITHDRAWAL.

9.1. Withdrawal by the contractor

9.1.1. Without prejudice to the terms set forth in Article 9.2 "WITHDRAWAL" of the General Terms– General Part, the Contractor can withdraw from the Contract only where expressly provided for in the Contract in accordance with all the constrains specified herein.

9.2. Withdrawal of ENEL due to insolvency proceedings on the part of the Contractor.

9.2.1. Without prejudice to the terms set forth in Article 9.2. "WITHDRAWAL" of the General Terms– General Part, regarding the withdrawal of ENEL in other cases, in case the Contractor goes bankrupt or is subject to insolvency or receivership proceedings, the Contract will be terminated pursuant to Article 81 of Royal Decree. 267/1942 (bankruptcy law).

10. TERMINATION AND ENFORCEMENT IN CASE OF BREACH

10.1. Without prejudice to all the other cases expressly envisaged in the Contract and the terms set forth by the applicable law and in particular Article 9.3, "TERMINATION" of the General Terms – General Part, ENEL reserves the right to terminate the Contract, pursuant to and by effect of Article 1456 of the Italian Civil Code, in the following additional cases in which the Contractor and/or any subcontractors:

- fail to allow their skilled workers and working equipment to be identified or fail to allow ENEL staff and/ or third parties appointed by ENEL to gain access to their branches/workshops/warehouses or to the sites and working areas, to perform the checks envisaged by the Contract and/or by the law and/or refuse to allow ENEL to carry out these same checks, or even prevents them from doing so, in some way;
- have even only a pending insolvency procedure against them;
- use materials and equipment belonging to ENEL inappropriately or for purposes other than those established in the Contract;
- behave improperly when performing the services, in particular with regard to waste management;
- the services prove not to have been executed to the highest standards of good workmanship;
- fail to immediately notify ENEL, the Contract Manager, of any site inspections, inspections, accesses, reports or any other initiatives raised by the Criminal Investigation Department or other supervisory bodies regarding potential breaches of the environmental law, that they themselves, or one of their sub-contractors or auxiliary companies may have received, during the activities carried out on ENEL facilities or in any case performed on behalf of ENEL;
- prove not to comply with one of the duties envisaged by Article 19 below, in relation to waste management, without prejudice, in any case, to the right of ENEL to suspend the execution of the Contract.

10.2. In all cases of non-fulfilment, ENEL – at its sole discretion – can assign to the Contractor a term by which the same must ensure their compliance. If the Contract fails to envisage a different term, this will not be less than fifteen days. If said term is reached and the non-fulfilment has still not been resolved, ENEL, without prejudice to its right to terminate the Contract pursuant to and by effect of Article

1456 of the Italian Civil Code, can proceed in assigning the Contract to third parties, without prejudice to its right to claim compensation for any additional damages suffered. This assignment will be notified to the Contractor in breach, indicating the new terms of execution of the same and the relative amount.

In this case, the Contractor will only be liable for the payment of the amounts due for the activities that have been regularly executed, as indicated in the relative progress report, to be drawn up by both parties. This amount can be offset with any amounts owed by the Contractor as a penalty and/or additional damages/costs in any case associated with the advanced termination, such as, for example, those resulting from the establishment of a new Contract with third parties or the direct execution of the activities that form the subject of the Contract.

10.3. The enforcement of the Contract due to breach fails to exempt the Contractor from any additional responsibilities that may arise in connection with the advanced termination of the Contract.

10.4. Without prejudice to cases of wilful misconduct or gross negligence and should different provisions not have been set forth in the Contract, the liability of the Contractor for breach of the contractual obligations and the consequent obligation to compensate ENEL cannot exceed 100% of the value of the Contract.

11. PROTECTION OF THE ENVIRONMENT[3].

11.1. Without prejudice to the terms stated in Article 17 “GLOBAL COMPACT” of the General Terms and Conditions – General Part, in compliance with the principles of the environmental policy adopted by ENEL, the Contractor undertakes to implement all the precautions and measures necessary to protect the environment.

11.2. The Contractor must comply with all the applicable legislation regarding the environment and any other commitments associated with or formally undertaken by the same, and :

- show that they have identified and that they are aware of the implications connected with the applicable environmental law;
- provide, upon request, all the documentation that certifies their conformity with the applicable environmental legislation;
- show that they have procedures in force which allow them to maintain the essential requisites and their continuous compliance with the applicable law;
- have carried out a risk assessment, designed to identify all their processes and activities that could pose risks, including potential risks, with reference to the requirements of the applicable legislation and that they have adopted adequate measures to prevent these from occurring;
- promptly provide ENEL, when requested, with details about the environmental performances (e.g.: fuel consumptions, hazardous waste).

The Contractor must prepare a plan for the specific prevention and/or mitigation of the environmental impacts of the site and the activity.

This plan must be submitted to ENEL before the activities that are the subject of the Contract commence, and it must comply with the legislation in force and guarantee the highest standard of control, with a view to maintaining a high standard of environmental protection.

The Contractor must communicate to ENEL, within maximum 24 hours:

- any amendments or updates to the authorisations and/or permits, providing a copy of the new documentation issued by the competent authorities;
- proof of the checks and inspections carried out by the competent authorities and, in case of any breach of the same, the actions performed or planned in accordance with said authorities to restore the compliance with the law;
- communicate any environmental accidents or emergencies and the measures implemented to manage and resolve the event.

11.3. The Contractor must, insofar as it is applicable to the subject of the Contract, and without prejudice to the terms set forth in the Contract;

- use recycled (or partially recycled) materials or materials with a high level of recyclability, preventing the potential generation of waste; this is true in particular for the raw materials in general and the packaging materials; at least 80% of the weight of all the products used must, wherever possible, be composed of recyclable/recycled materials;
- guarantee that the elements used in the materials and equipment are not cancerogenic or chemically unstable;

[3] This clause “PROTECTION OF THE ENVIRONMENT” only applies to works, services - including operations performed on behalf of ENEL and/or at ENEL offices/sites-, supplies - only when these entail installation/assembly activities, the supervision of works, or loading/unloading activities and to supplies of hazardous substances/chemical reagents. Additionally, this Article is also applicable to any service or supply considered by ENEL to carry a High or Medium Environmental Risk.

- comply with the provisions and restrictions relative to the sale of hazardous substances and preparations as envisaged by the legislation in force; in particular, proof of the absence of PCBs in oil as well as the absence of CFCs, HCFCs, halons, etc. must be provided;
- provide their staff with clothing that is free from toxic substances;
- use batteries that do not contain mercury and have small quantities of heavy metals;
- sort and recover all the metal and non-metal materials such as PVC, PEAD, PP, demolished materials etc. used during the execution of the Contract, so that these can be recycled;
- minimise consumptions of energy, water and commodities throughout the life cycle of the service/product, related to the optimisation of the return;
- prevent leaks, spillages and pollution of the soils, waterways and canals;
- at the end of the activities, the Contractor must leave the working area clean, free from waste, debris, etc., as the collection and transportation of the waste are at the Contractor's expense;
- minimise noise, atmospheric and electromagnetic emissions, and in particular, for example:
  - use production processes that do not envisage the use of pollutants;
  - use eco-friendly paints;
  - use products that do not contain harmful chemical additives which could contaminate the environment;
  - use, in general, non-polluting products under ecological brands (etc.: Ecolabel, Blue Angel, Nordic Swan, FSC certificates, etc.);
  - manage the maintenance of its tools and machinery to prevent them from deteriorating and therefore compromising the environmental performances (vibrations, noise emissions, atmospheric emissions);
- arrange to deliver the goods using methods envisaging packaging that:
  - does not contain chlorinated plastic;
  - is made with materials that render it suitable for recycling/reuse;
  - is not made of halogenated synthetic materials;
  - can be managed with the recycling system;
- use means of transport that envisage the following procedures:
  - use pallets certified by FSC for the movement and transportation of the materials;
  - use means of transport compliant with the most recent European standards regarding the reduction of emissions;
  - ensure the correct collection and management of lubricants and used tyres;
  - use regenerated lubricants and eco-friendly tyres;
- raise the awareness of all the staff employed for any reason during the execution of the Contract regarding the need to behave in such a way as to reduce the environmental impact.

11.4. The Contractor undertakes to prove, upon ENEL's request, that they have ecological labels for the materials used and that they can provide specific documentation issued by recognised authorities.

11.5. ENEL reserves the right to monitor or check that the Contractor is correctly managing its waste.

11.6. The Contractor must guarantee that the staff know and understand the requisites and laws in force regarding environmental protection which are necessary in order to perform the work. They must demonstrate that their staff has undergone adequate theory-based and practical training designed to ensure that the works are carried out correctly and limit the risk of accidents with environmental consequences; the training must comply with the terms set forth in the environmental management system envisaged in the site which is the subject of the works.

11.7. The Contractor undertakes:

- to immediately inform ENEL of any environmental accident that may occur during the execution of the services;
- to submit a written report on the accident and the relative causes to ENEL;
- in case an environmental accident occurs, to follow all the instructions/indications provided by ENEL.

11.8. ENEL - at its own sole discretion - is entitled to automatically terminate the Contract in case of any breach on the part of the Contractor and/or the subcontractor, of even only one of the provisions of the legislation in force regarding environmental protection and any further provisions regarding the environment expressly envisaged by the Contract.

11.9. Without prejudice to that specified above, should the Contractor infringe or fail to comply with any of the provisions of this Article, ENEL can, at its sole discretion, suspend the works, charging the costs to the Contractor, to prevent the occurrence or extension of environmental damage.

All the costs for the implementation of the above-mentioned environmental policy are to be considered as already included in the contract prices.

12. CODE OF ETHICS

12.1. General information

12.1.1. The ENEL group , when conducting its business and managing its relationships, refers to the principles contained in its own Code of Ethics, in the Zero Tolerance plan against corruption, in the Organizational Model adopted pursuant to Italian Legislative Decree 231/2001 and in the Human Rights Policy which can be consulted at the link:

http://globalprocurement.enel.com/it-IT/documents/documentation/.

The Contractor, when conducting its own business and managing its relationships with third parties, upholds equivalent principles.

12.2. Declaration of Conflict of interest.

12.2.1. The Contractor, also with reference to the commitments undertaken in Article 18.2. "CONFLICT OF INTEREST" of the General Terms– General Part, undertakes to ensure that the relative statement issued to ENEL is constantly updated.

12.3. Declaration *ex* special part "D crimes against the personality" [4].

12.3.1. The Contractor, with reference to the commitments undertaken in Article 11.1. "GENERAL INFORMATION" of the General Terms– General Part regarding the protection of the right of publicity, in cases where they have not already issued the same to ENEL and providing that there are no amendments to be notified, undertakes to sign the relative statement as per Attachment 1 ANNEX ITALY of this document.

12.4. Express termination clause for the crimes contemplated by Legislative Decree 231/01.

12.4.1. With reference to Article 11.1 "GENERAL INFORMATION" of the General Terms– General Part and the principles expressed therein and to the relative commitments undertaken by the Contractor to prevent corruption**,** should it have been ascertained, with the passing of a definitive sentence, that the Contractor[5] has committed administrative crimes and/or one or more of the crimes contemplated by Legislative Decree 231/2001, ENEL will be justified in terminating the Contract with immediate effect, pursuant to and by effect of Article 1456 of the Italian Civil Code, without prejudice to the right to claim compensation for damages that may be caused to any company of the Group such as, for example, those deriving from the application of sanctions, envisaged by the above-mentioned Decree.

12.5. Confidentiality statement and Regulations for the use of the ENEL computer systems[6].

12.5.1. The Contractor undertakes to comply with the duties envisaged in Attachment 2 ANNEX ITALY hereto. They also undertake to submit to ENEL the statements as per the above-mentioned Attachment, duly signed, where these have not already been issued and providing that there are no amendments to be notified.

12.6. Integrity clause.

a) With the bid submission and/or the acceptance of the Contract, the Bidder/Contractor[7] 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;
- [8]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;
- [8] 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;

[4] The statement is required in the following cases:

(1) establishment of contracts with Contractors that use staff from countries outside the European Community;

(2) establishment of contracts with Internet Providers regarding the supply of digital contents.

[5]The Legal Entity.

[6] This clause is applicable to contracts that envisage the granting of access to ENEL premises and/or the accessing and processing of data and information of the ENEL group as well as the use, by the Contractor, of the ENEL computer systems.

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

[8] For itself and for the persons listed in note 7.

- to take note and authorise 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, at any time, in consideration of the necessary existence of fiduciary duties with the Company involved.

b) The Bidder/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 purpose of assessment of the professional conduct of the Bidder/Contractor itself and of the Company concerned.

13. PERSONAL DATA PROTECTION

13.1 Privacy notice regarding personal data processed by parties for the purposes of this contract

13.1.1. For all definitions concerning personal data, reference is made to terms and definitions made in EU Regulation 2016/679 (hereafter GDPR), as well as to the implementing legislation and any other current legislation in force

13.1.2. Parties are informed that personal data are reciprocally acquired during the assignement of the Contract, and processed for the management and execution of the Contract, or to comply with applicable laws. Personal data will be collected and processed using automated means and / or in paper forms 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..

13.1.3. In this respect, it should be noted that:

- the Data Controller is the Client Company of the ENEL Group[9] in the person of its legal representative *pro tempore* (hereinafter "ENEL");
- The data subject is the natural person participating in the awarding procedure, whose personal data are processed for the purposes of stipulation, management and execution of the Contract (hereafter the Data Subject);
- Personal data processed may be transferred to third parties, i.e. to companies subject to management and coordination or connected with ENEL S.p.A., or to other third parties. Third parties may be appointed by the Data Controller as Data Processor;
- Data Subjects are 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;
- Data Subject are entitled to lodge a complaint to the Italian Data Protection Authority, with registered office in Piazza Venezia 11 – 00187 ; Rome. Tel. (+39) 06.696771, email: garante@gpdp.it;
- 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.

13.2. Appointment of the Contractor as Personal Data Processor

13.2.1.

Upon signing of the Contract, and for its entire duration, the ENEL Group Client Company, as Data Controller, appoints the Contractor, who accepts, as Personal Data Processor, pursuant to and for the purposes of Article 28 of the GDPR.

If the Contractor 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 all appointed as Data Processors.

13.2.2.

The Contractor undertakes to carry out personal data processing operations in compliance with the obligations imposed by the GDPR and the instructions thereafter issued by ENEL, which will monitor thorough compliance with the GDPR obligations and the above-mentioned instructions.

It is agreed that Enel has the unilateral right to terminate the Contract under Article 1456 Italian Civil Code if the Contractor is in default of the obligations pursuant with this paragraph.

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

13.2.1. Duties and instructions

13.2.1.1. The Contractor, 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 as follows::

a) It must only process personal data according to ENEL instructions, as documented in Attachment GDPR 1 specifying type of data processed and the categories of Data Subjects;

b) It will have to appoint Authorized Persons ("Authorized Persons") to carry out its data processing operations in IT or paper files, including simple data visualization, by using the specific template provided by ENEL (Attachment GDPR 2) Before starting the activities covered by the Contract or otherwise by the date specifically communicated by ENEL, the Contractor will also send ENEL a statement concerning the list of appointed employees/collaborators as "Authorized Persons" according to the template provided by ENEL (Attachment GDPR 3);

c) It must ensure that Authorized Persons comply with GDPR obligations and Enel instructions and maintain integrity and confidentiality of the personal data during the execution of the Contract and do not to communicate them to third parties, unless expressly authorised to do so by ENEL and except for the cases expressly envisaged by the law; ENEL reserves itself the right to request the Contractor 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) It must adopt all the security measures as set forth in Article 32 of the GDPR, as well as all other preventive measures dictated by the experience designed in order to avoid personal data processing not allowed or not compliant with the purposes for which the data are processed; it must also ensure effective collaboration in implementing these measures in the notification and communication of any personal data breach and in assessing the data protection impact assessment when requested by ENEL;

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

f) It may transfer personal data to a third country or to an international organisation located outside the European Union only in the cases envisaged and under the conditions defined by the GDPR, unless otherly required by law of the European Union or the national law to which the Contractor is subject. In this case, the Contractor undertakes to inform promptly ENEL about this conflicting 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 Contractor undertakes to support ENEL in deploying its own appropriate technical and organisational measures, to the extent to which this is possible, in order to let ENEL to fulfill it's duty to respond data subject's request to exercise their rights;

h) 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 its role as Data Processor;

i) It 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 it should erase also the existing copies, unless the law of the European Union or its member States envisages that personal data have to be stored; proof of accomplished erasure has to be provided to Enel;

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

k) It 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;

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

m) It must cooperate with ENEL by making freely available all necessary information in order to allow Enel compliancewith Articles 33 and 34 of the GDPR, including up-to-date and valid certifications;

n) According to Article 30of the GDPR, it must keep a data record of the processing activities carried out on behalf of ENEL, which must be exhibited upon request of ENEL when subject to legal obligations under articles 33 and 34 of the GDPR.

13.2.1.2. It is forbidden to the Contractor to process personal data for purposes other than the execution of the Contract. In particular, where it is not necessary for the execution of the Contract, it is forbidden for the Contractor to make, by way of example but not exhaustive, to massively extract personal data, also through the use of "RPA - Robotic Process Automation" (or "automata"), unless previously authorized by the Contractor.

13.2.2 Compensation and Liability

13.2.2.1

Pursuant to Article 82 of the GDPR, the Contractor will be liable for damages caused by the processing if it has failed to comply with the duties and obligations aforementioned or has acted in a different or contrary way to ENEL's instructions.

The Contractor will also be liable in the first place with ENEL and its data subjects if any Data Processor appointed by the Contractor to execute data processing pursuant to the Contract fails to fulfil its obligations with the GDPR or the Contractor' instructions .

13.2.2.2

In the event of further damages incurred by ENEL as a result of the conduct of the Contractor or one of its Data Processors, ENEL reserves the right to request further compensation that will be proportionate to the damages suffered.

ENEL or the Contractor are exempt from all liability if they can prove that the damaging event is in not in any way ascribable to them.

13.2.3 Duration

13.2.3.1

The above-mentioned appointment as Data Processor will be automatically revoked to the Contractor upon exipration 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.

13.2.4 ther Data Processors (or Sub Data Processors)

13.2.4.1.

If, for specific processing activities, the Contractor intends to involve in the execution of the Contract Data Processors outside its own organization, these must be appointed as Sub Data Processors pursuant to Article 28 paragraph 4 of the GDPR (hereinafter indifferently Other Processors or Sub Data Processor). The Sub Data Processors must comply with the same obligations that this Contract carries out on the Data Processor (Attachment GDPR 4). In particular, in compliance with letters b) and c) of paragraph 13.2.1 "Duties and instructions", each Sub Data Processor shall in turn appoint any resources used in the processing as "Authorized Persons" for processing personal data, using possibly the template and the related instructions in Attachment GDPR 7.

13.2.4.2. Before starting the activities covered by the Contract or otherwise by the date specifically communicated by ENEL, the Sub Data Processor will also send ENEL its own statement 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 8);

Upon signing of the Contract the Sub Data Processors are thereby authorized (Attachment GDPR 5) to process personal Data.

13.2.4.3. If the Contractor, for recognizable and reasonable reasons, intends to entrust services to Sub Data Processors other those included in the first list referred to in Attachment GDPR 5, it must request prior authorization to Enel for such appointments, using template in Attachemnt GDPR 6 or equivalent form. Enel has the right to issue a general authorization valid for the entire duration of the Contract for allowing all Sub Data Processor to process its personal data or can issue specific and individual authorizations, depending upon the nature of the services and the duties defined forth in Article 28 of the GDPR.

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

13.2.4.5. If Sub Data Processors process data in the United States, if subject to US law, the Contractor 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 for itself and its Sub Data Processors.

13.2.4.6. If a Sub Data Processor belong to the Contractor'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 Sub Data Processor.

13.2.4.7. Should the Sub Data Processors intend to process personal data in countries considered inadequate in relation to the GDPR, the Contractor 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, ENEL confers to the Contractor, as Data Processor established in the European Union, a specific mandate with representation so that it can sign the above-mentioned Standard Contract Clauses.

13.2.5 System administrators

13.2.5.1. Since Contractor’s staff and/or of its Sub Data Processors., should any be authorised, could carry out functions ascribable to the role of “system administrator” as per current legislation, the Contractor undertakes to provide, upon ENEL's request, the list of its and Sub Data Processors staff and employees authorised to act as “system administrators” and of all those people who could potentially intervene on the personal data belonging to ENEL (Data Processor System Administrators)..

13.2.5.2. The Contractor also undertakes to keep a register of the logs of access, disconnection and attempted access of its Data Processor System Administrators) and to save those information for a period of six months, with the commitment to submit them to ENEL within 3 calendar days in the specified format, upon receipt of a request in writing.

SECTION II - WORKS, SERVICES, SUPPLIES WITH INSTALLATION.

14. METHODS OF PERFORMING THE ACTIVITIES.

14.1. Should the activities be performed near – and/or lead to interference with – plant (electrical, telephone, gas, water and waste water, etc.) and/or infrastructures (roads, canals, railway lines and other similar elements) belonging to ENEL or to third parties, the Contractor, before commencing the execution of the services, must take initiative, integrating and checking the information, floor plans, and basic maps received by ENEL, recovering the necessary and useful information regarding the presence and layouts of the plant and infrastructures and also identify those located fully or partially beneath ground level.

14.2. The Contractor must comply with the provisions received from time to time and with the procedures in force at ENEL or on the premises of the third party owners, in line with the laws in force and the directives issued by the competent Authorities.

14.3. The Contractor shall be liable for any delays in redelivering the plant and restoring it to service in line with pre-established times and plans, accepting responsibility for any damages caused to third parties, the owners and to ENEL.

15. EXECUTION OF WORKS WITH STAFF ON ENEL PREMISES.

15.1. Should the Contract envisage the presence (even occasional) of workers engaged in the execution of the activities that form the subject of the Contract, for various reasons, on the premises of ENEL, the Contractor must personally carry out a technical site inspection at the locations in which these workers will work, before the activities commence.

15.2. The Contractor will receive from ENEL the documentation regarding the risk assessment and the prevention and protection measures for those locations and will collaborate with the same to implement the terms set forth by the legislation on prevention, protection and safety at work.

16. CONTRACTOR'S OCCUPATIONAL HEALTH AND SAFETY OBLIGATIONS.

16.1. Provisions regarding the health and safety of the workers.

16.1.1. The Contractor, when performing the activities that form the subject of the Contract, must ensure the compliance of all the provisions of the laws, regulations and contracts in force regarding the health and safety of the workers as per Legislative Decree no. 81/2008 as amended and all the specific applicable standards.

The Contractor must also:

- appoint a supervisor from among its staff pursuant to Article 2 paragraph 1 letter e) of Legislative Decree 81/08 as amended;
- employ people who have suitable qualifications and certificates for the activities to be performed, as envisaged by the individual national legislations and by the ENEL procedures;
- use machinery, equipment and devices that comply with the legislation in force and with good practices and which have been subject to the regular checks required by the legislation;
- refrain from tampering with the temporary works and protections of ENEL or of other contractors
- only use machinery, equipment and devices that have previously been communicated to ENEL;
- not to use machinery, equipment and devices of ENEL without advance authorisation to do so;
- keep the work areas reasonably clean and tidy during the activities for which they are responsible;
- comply with the provisions contained:

➢ in case of works *ex* Title IV of Article 26 of Legislative Decree 81/08 as amended:

- in their own Risk Assessment Document (DVR) with reference to the specific risks of the activities that form the subject of the Contract;
- in the Single Document on the Assessment of the Risks from Interference (DUVRI);

➢ in case of works *ex* Title IV of Legislative Decree 81/08 as amended:

- in the Safety and Coordination Plan (SCP);
- in its Operational Safety Plan (POS);

participate in the meetings of cooperation and coordination held by ENEL.

16.2. Instructions regarding first aid, fire prevention and emergency management.

16.2.1. The Contractor and any subcontractors must comply with the terms set forth by the law regarding first aid, fire prevention and emergency management.

16.3. Working with electricity

16.3.1. As set forth by Legislative Decree 81/08 as amended and integrated by IEC Standards EN 50110 and 11/27, the Contractor and any subcontractors must assess, for each individual activity of theirs, the electrical risks.

16.3.2. For activities performed on off-line installations, the Contractor's supervisor must be classified as a Qualified Person (PES). If the staff member who is operating is classified as an Ordinary Person (PEC) the supervisor, or a person classified as an Instructed Person (PAV) must constantly watch over the activities of the same.

16.3.3. For activities performed on live installations on systems classified as Categories 0 and 1, pursuant to IEC Standards EN 50110 and 11/27, the supervisor must be classified as a Qualified Person and have been deemed qualified to carry out works on live Category 0 and I systems. Staff must be classified as PES or PAV and have been deemed qualified to perform works on live Category 0 and I systems.

16.3.4. The Contractor is strictly forbidden from commencing the activities, before ENEL has delivered the electrical installation that is the subject of such activity to the same.

16.4. Use of chemical substances.

16.4.1. The Contractor must not bring hazardous chemical substances into the ENEL sites without ENEL's prior authorisation.

16.5. Confined spaces

16.5.1. In case of activities to be performed in environments in which there is a suspected risk of pollution or in confined spaces (for example tanks, silos, galleries, wells, etc.), in order to prove the effective capabilities of the staff who will carry out the works, before the execution of the activities, the Contractor/subcontractor must provide a list of the names of the workers who will perform said activities, accompanied by suitable documentation certifying that said work force has the requisites prescribed by Presidential Decree 177/2011.

16.5.2. Should the work be subcontracted, the subcontractor must be authorised by ENEL and certified pursuant to Title VIII Chapter 1 of Legislative Decree 276/03.

16.6. Temporary and mobile sites.

16.6.1. Before the works commence, the Contractor and any subcontractors, in relation to the contents of the documents regarding safety submitted to them must draft and send the Operational Safety Plan (POS) for the individual site in which the works will take place, as set forth in Article 89 letter h) of Legislative Decree 81/08 as amended.

16.6.2. The Contractor and any subcontractors must present their own Operational Safety Plan (POS) reasonably in advance of the commencement of the relative works to enable the Works Coordinator to verify the suitability of the POS and ensure its coherence with the Safety and Coordination Plan (PSC).

The POS must contain the minimum elements identified by point 3.2 of Annex XV of Legislative Decree 81/08

16.7. Penalties for breaches of the health and safety legislation.

16.7.1. With reference to Article 11.2. “SANCTIONS FOR BREACHES OF THE LEGISLATION ON OCCUPATIONAL HEALTH AND SAFETY” of the General Terms– General Part, ENEL, for each non-compliance committed by the Contractor regarding the protection of OCCUPATIONAL HEALTH AND SAFETY, ENEL is entitled to apply, notifying the Contractor by registered letter with return receipt of delivery, a pecuniary penalty of:

- Euro 500.00 (five hundred/00) for each “SERIOUS” non-compliance [10]
- Euro 1.000,00 (one thousand/00) for each “VERY SERIOUS” non-compliance[11]

16.7.2. Should the "SERIOUS", "VERY SERIOUS" and "GRIEVOUS" non-compliances cause work injuries or in any case damage to persons, ENEL reserves the right, with its decision being final, to apply – in relation to the seriousness of the violation and/or of the injury and/or of the damage to the person - a pecuniary penalty of up to 2% of the total contractual amount and, in any case, of no less than € 1,000.00 (one thousand/00).

16.8. Asbestos.

16.8.1. The Contractor , during the execution of the activities that form the subject of the Contract, undertakes not to use any materials and objects containing asbestos. Should asbestos be detected in the assigned work area or should there be a suspicion that it may be present, the Contractor must stop the activities and notify the competent ENEL supervisor accordingly, in order to ensure that the situation is managed correctly.

17. CONTROLS

17.1. ENEL is entitled to control and verify that the Contractor accurately fulfils all the duties undertaken by the same when signing the Contract, and all and any additional requirements envisaged by ENEL during the execution of the same.

[10] As classified in the table "List of Serious and Very Serious breaches" as per Article 11.2 of the General Terms

[11] As classified in the table "List of Serious and Very Serious breaches" as per Article 11.2 of the General Terms

17.2. Should, at the outcome of these controls, the Contractor fail to submit in writing any disputes in relation to the decisions made by ENEL within ten days from receipt of the same, these decisions will be considered as accepted in full and the Contractor will lose its right to submit any reservations.

18. RESERVATIONS.

18.1. All and any reservations that the Contractor may intend to formulate, for any reason, must only be submitted, under penalty of invalidation, by signing the accounting document with reservation under the update relative to the period in which the event that determined the reservation occurred.

18.2. The Contractor must also state, under penalty of invalidation, the reservations submitted on the accounting register, and on the reports confirming receipt.

18.3. The Contractor is obliged to express such reservations, notifying ENEL - within fifteen days from the signature with reservation of the accounting document- of the reasons for such reservations and providing specific details of any recompense to which it believes it is entitled.

18.4. Obviously no new reservations other than those relative to facts regarding the latest update will be permitted.

18.5. If the Contractor signs the latest update of the accounting document without reconfirming the previous reservations, all the previous situations relative to the works and services that form the subject of the Contract, will be considered as having been definitively accepted by the same, and the relative reservations will be deemed as having expired. Equally, if the Contractor fails to state any reservations regarding to the latest temporary situation, this will also be considered as having been definitively accepted.

18.6. Except the cases in which ENEL deems it suitable to anticipate the review of the same, the reservations presented in the above-mentioned methods and terms will be examined after the Contractor has signed the report confirming their definitive acceptance of the works.

19. MANAGEMENT OF THE WASTE GENERATED BY THE WORKS OR SERVICES FORMING THE SUBJECT OF THE CONTRACT.

19.1. The waste generated by the activities that form the subject of the contract and assigned to the Contractor is classified as "Special waste"; this must be managed in compliance with the provisions of the law in force and all the terms set forth in the Contract.

If envisaged in the Contract, the waste must be conferred by the Contractor, at their own expense and under their own responsibility, to parties authorised to perform recycling activities or, should this not be possible, to parties authorised to dispose of the same.

In particular, the Contractor will be legally liable for the correct management of any temporary waste deposits and for correctly completing and keeping the environmental documents.

19.2 In the case described in the previous point, unless differently established within the Contract, the Contractor can under no circumstances set up temporary waste deposits on the sites involved in the execution of the activities which form the subject of the Contract.

19.3 The Contractor, as the producer of the waste generated by the activities that form the subject of the Contract, is responsible for all the activities connected to the correct management of the waste, including packing activities.

Specifically, the Contractor, in order to perform the activity related to the management of the waste must:

a) be registered in the National Register of Environmental Managers, pursuant to Article 212 of Legislative Decree 152/2006;

b) have provided ENEL with the following when submitting the offer:

- a copy of their entry in the Register together with a copy of the receipts that attest to the payment of the annual fees, on the relative due dates;
- copy of their registration in the waste traceability system (SISTRI), where applicable;
- registration in the "White Lists", where required;

c) confer the waste produced to parties authorised to recycle and/or dispose of the same;

d) provide ENEL with a copy of their own authorisation to recycle or dispose of waste, if they are the owner of a recycling or disposal plant which they intend to use for the conferral of the waste produced during their activity;

e) provide ENEL with a list of the potential parties to whom the waste produced during the execution of the activities which form the subject of the contract may be conferred, should the recycling or disposal activities be performed by plants owned by third parties, attaching a copy of the relative authorisations;

f) promptly notify ENEL of any updates or amendments made to the deeds of registration in the Register, providing the updated documentation, and any decisions made by the competent authorities that imply restrictions or revocations of these;

g) deliver to ENEL, before the execution of any activity requested by ENEL that forms the subject of the above-mentioned Contract, a statement confirming the validity and effectiveness of the above-mentioned authorisations

and registrations, which must specify, among other things, that no provisions revoking or suspending the same have been, or are being, implemented by the competent Authorities.

19.4. Should the Contractor not perform the activities of waste collection, transportation and delivery in their own right, these must be assigned under subcontract, in compliance with the relevant legislation in force and subject to the express authorisation of ENEL .

For the purpose of authorising the subcontract, the Contractor must also provide ENEL with:

- a copy of the entry in the National Register of Environmental Managers for the party/parties who will carry out the waste collection and transportation activities;
- copy of the registration in the waste traceability system (SISTRI), where applicable;
- the list of plants to which the waste produced during the execution of the contract will be delivered and the relative authorisations;
- a list of the types of waste generated.

19.5. Should the Contractor use a broker, for the management of the waste, in addition to the documentation listed above, they must also provide ENEL with a copy of the broker's entry in the National Register of Environmental Managers.

19.6. The waste produced by the Contractor can only be deposited in the areas assigned by ENEL, in compliance with the provisions set forth governing the temporary holding of waste. ENEL

Where weighing systems are present, the waste must be weighed under the supervision of ENEL .

19.7. The Contractor, before every transportation, must deliver to ENEL the copy of the first copy of the Identification Form, also by Certified Public Email (PEC).

On a monthly basis, or in any case when the Work Progress Reports (SALs) are drawn up - and in any case in compliance with the maximum times envisaged by the sector-specific legislation for submitting the documentation for the transportation of the waste - for the waste generated by the activities carried out in the period and/or registered in the accounting system in the individual Work progress Reports, the Contractor must provide ENEL with a copy - also by way of Certified Public Email (PEC) - of the fourth copy of the Waste Identification Form (FIR), countersigned by the recipient or the copy of the documentation envisaged in case of cross-border shipments.

The payments of the individual SALs and in any case of the final SAL are subject to receipt of the copy of the first and fourth copy of the Waste Identification Form. Before the final SAL is issued by ENEL, the Contractor must also declare that they have arranged to manage the waste in compliance with the law, also indicating the type of waste (CER) managed.

ENEL can ask the Contractor to provide a copy of the waste management register at any time and the Contractor cannot refuse to do so.

19.8. Where envisaged, with reference to the management of earth and rocks deriving from excavation activities and classified as by-products, the Contractor must provide a copy of the self-certifications submitted to the Regional Environmental Protection Agency for (ARPA), regarding the compliance with the criteria set in relation to the reuse and full use of excavated earthen materials.

19.9. ENEL reserves the right to perform random checks.

19.10. With reference to the waste for which ENEL is identified as the producer, the Contractor or any subcontractors of the same authorised by ENEL , to whom ENEL will assign - in its capacity as intermediary, transporter, recycler and/or disposer - the management of its waste, undertake to perform the activities in compliance with the legal provisions in force and all the obligations envisaged in the Contract. In particular, the Contractor and any subcontractors of the same must ensure compliance with the provisions of this Article, insofar as they are applicable.

20. TERMINATION REGULATIONS

20.1. Without prejudice to the terms set forth in Article 9. “SUSPENSION, WITHDRAWAL AND TERMINATION” of the General Terms– General Part and the terms established in Article 10 above. “TERMINATION AND EXECUTION IN DEFAULT, in all cases of termination with regard to the Contract, ENEL notifies the Contractor of the date and the methods with which the delivery operations of the works and the transfer of possession of the sites must take place. The Contractor must deliver the works immediately, *as is*, while ENEL is entitled to take all or part of the plant on site, the temporary works and materials of the Contractor.

20.2. The Contractor must pick up the machinery, equipment and working tools belonging to the same which ENEL does not intend to use, remaining fully liable for shutting down the sites, even in several stages, in compliance with the indications provided for this purpose by ENEL, with 30 days' prior notice.

20.3. The above is true in any case without prejudice to ENEL's right to claim damage compensation. Should any of the amounts described in this Article be acknowledged as being owed to the Contractor or as having been paid to the same, this does not imply any waiver of the Contractor's right to claim damage compensation.

21. SAFEKEEPING.

21.1. From the delivery date of the works until the acceptance of the same by ENEL, and limited to the materials used for which ENEL has benefited from the right of use, the Contractor is solely liable for the safekeeping of the sites, tools, materials and the works in progress, also during any periods of suspension of the works.

21.2. Additionally, the Contractor is also responsible for the preservation, safekeeping and use of the materials they need to engage, in particular those provided by ENEL, from the date on which they are received, indemnifying ENEL from all relative liability, including any damage to third parties.

22. ACCESS TO SITES AND WORK AREAS

22.1. The Contractor will be liable for all the tasks and costs of gaining access to the sites and the work areas, as well as the design, installation, construction, adjustment and maintenance in perfect running order of suitable site plant and temporary works required for the execution of works, jobs and interventions.

22.2 Any accesses to the site by any party (subcontractors, service providers etc.) must be expressly authorised by ENEL.

23. SITE SIGNAGE.

23.1. The Contractor, as well as any subcontractors/sub-assignees, must arrange to signpost the sites using site signage that complies with the layouts recommended by ENEL.

The Contractor, as well as any subcontractors/sub assignees, must also install, in full view and for the entire duration of the works, the safety and hazard signage required by the health and safety at work and traffic circulation laws in force.

The signs, in the required quantities. will be procured by the Contractor at their own expense and under their own responsibility.

24. TRANSPORTATION, WAREHOUSING AND DEPOSITS.

24.1. The Contractor must arrange to transport all the materials, equipment and machinery required for the execution of the contracted works within the site, including the loading and unloading operations, and depositing and storage tasks in the sites.

25. SITE SHUT-DOWN

25.1. In the period between the date on which the works are completed and that on which ENEL accepts the same, the Contractor must progressively shut the site down, in line with a plan agreed upon previously with ENEL, arranging to demolish the temporary works, transport and dispose of the by-products, leaving the used areas clear and tidy in order to prevent any damage occurring to people and things.

Attachment 1 annex italy

Declaration *ex* special part "D crimes against the personality" .

HUMAN RIGHTS DECLARATION (Company)

The Company, in the person of its legal representative, …… in the awareness that making an untruthful statement will justify ENEL in terminating the Contract and claiming damage compensation,

declares:

that **it has been / has not been** (cross out the option that does not apply) investigated in the last 5 years in legal proceedings relative to the following crimes against the personality: subjection to or maintenance of people in slavery or servitude, child prostitution, child pornography, possession of paedopornographic material, tourist initiatives designed to exploit child prostitution, human trafficking, the buying and selling of slaves.

The undersigned company undertakes to communicate promptly to ENEL any changes to the information conveyed in this statement. Additionally, it is aware that ENEL can, at any time request proof of the contents of this declaration and hereby undertakes to provide appropriate supporting documentation.

Yours faithfully,

Date, ……

Company stamp Signature of legal representative

****

HUMAN RIGHTS DECLARATION (Natural Person)

The undersigned…….. in the awareness that making an untruthful statement will justify ENEL in terminating the Contract and claiming damage compensation,

declares:

that it has been / has not been (cross out the option that does not apply) investigated in the last 5 years in legal proceedings relative to the following crimes against the personality: subjection to or maintenance of people in slavery or servitude, child prostitution, child pornography, possession of paedopornographic material, tourist initiatives designed to exploit child prostitution, human trafficking, the buying and selling of slaves.

The undersigned undertakes to communicate promptly to ENEL any changes to the information conveyed in this statement. It is also aware that ENEL may at any time request proof of the contents of this declaration and hereby undertakes to provide appropriate documentation.

Yours faithfully,

Date, …..

Stamp Signature

Attachment 2 annex italy

STATEMENT OF CONFIDENTIALITY

CONTRACT NO. …… OF……

SUBJECT: ……

The undersigned:

_____

(first name and surname of the declarant)

☐ Natural person (only tick if the Contract in question is not in the name of a company)

(only tick if the Contract in question is in the name of a company)

☐ Owner

☐ Legal Representative

of _____

(Name/Company Name)

DECLARES:

- that the list of all those who will be able to access the premises of ENEL for purposes related to the Contract and/or access and process data and information of the ENEL group is as follows:

  1) Mr .....

  (Surname, First name)

  2) Mr .....

  (Surname, First name)

- that each of the persons listed above has signed the appropriate individual confidentiality clause attached hereto;
- that the reference person appointed to keep the list described above constantly updated is Mr_____ email_____ Tel._____ Fax_____

Attached no. ___ individual confidentiality clauses

Date _____

The Declarant

……

(Stamp and Signature)

INDIVIDUAL STATEMENT OF CONFIDENTIALITY

CONTRACT NO. ……..……..**OF**……..……

SUBJECT: ……..……

……..……

The undersigned……..……

born in ..... (.....), on ……..……..……

to be completed if the Contract in question is in the name of a

☐ employee

☐ consultant

} of the company ……..……

in relation to the above Contract, undertakes:

- not to disseminate or communicate to third parties the information collected, the opinions, the relative studies carried out, and any elements that may have been made available by ENEL for the execution of the above-mentioned Contract and to only use this information for the purposes of said Contract, except in cases in which the undersigned party must comply with the legal obligations or with requests from the Public Authorities which it cannot legitimately refuse;
- to view and carefully observe the recommendations for the security of the data specified in attachment hereto, and in case of using the IT systems provided by ENEL, to exercise the maximum diligence when keeping all the paper and/or digital media acquired or produced during the execution of the activity.

Information disclosed by ENEL itself, i.e. available in official documents, is excluded from such confidentiality obligations.

The confidentiality obligations remain effective **for a period of 5 years** from the expiry of this appointment, also in cases of withdrawal and direct and indirect termination of the relationship with ENEL based on the Contract.

For acceptance

Signature

Date: ……..……

Security rules for use of ENEL computer systems

The IT systems owned by the ENEL group must be accessed and used in compliance with the following security rules:

- the user credentials for the IT systems of ENEL must only be used by the user. The relative password must be kept strictly secret and changed at least every 60 days;
- the access to the IT system must be limited to the instrumental components for the execution of the activities envisaged by the appointment, even if the security measures implemented fail to prevent other components from gaining access. Users cannot use any network services or connect equipment other than those necessary for the execution of the jobs;
- the operations performed using the IT systems of ENEL must not breach the national laws or the provisions of international legislation;
- the workstation used for the execution of the jobs (fixed and/or portable) must not be used to connect to Internet in ways other than those that may be provided by ENEL;
- Personal laptop computers can only be connected to the ENEL data network if equipped with updated anti-virus software. In particular, users must adopt all possible counter measures designed to prevent the dissemination of viruses, worms, hoaxes, trojans and other illegal software that could interrupt the IT service;
- the texts and/or images created/sent using the IT systems of ENEL must not be offensive and/or inappropriate;
- any email accounts provided for the use of the user must not be used for “spamming” operations or to forward chain letters.

In relation to the instructions specified above, ENEL reserves the right to prevent any improper uses of its IT infrastructures, without prejudice to the duty to comply with the terms set forth by the laws in force. ENEL also reserves the right to report to the competent Court Authority any breaches that may constitute a crime.

Attachment 3 annex italy

List of the names of the Sub-processors

COMPANY	PRODUCT OR SERVICES	TYPE OR CATEGORY OF DATA PROCESSED	ADDRESS

GDPR ATTACHMENTS (FROM ATTACHMENT 1 TO ATTACHMENT 8)

ATTACHMENT 1 GDPR

Description of the personal data processing

With reference to Article 13 of Annex VII and to Order Letter no. …… and in particular to the appointment of the company [•] as Data Processor, with this attachment the Data Controller means to identify types of data and categories of data subjects related to the abovementioned contract.

A. Type of Personal Data

- **Biographical data**[12] □
- **Special categories of personal data**[13] □

- **Judicial data** □
- **Personal Economic & Financial Data** □
- **Data related to contracts with customers (e.g. POD, PDR)** □
- **Other** _____

B. Categories of Data Subjects

- **Customers** □
- **Employees** □
- **Suppliers** □
- **Shareholders** □
- **Other** _____

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

[13] these include 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: **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 Data 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 [•], hereinafter "Data Controller" ;
- 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

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, which means any operation, even if only for consultation, relating to personal data stored in IT and/or paper files held by the undersigned Company as Data Processor and/or by the 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 to you in relation to processing personal data.

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 consent collection stage must be preceded by a specific privacy notice and by the release 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 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 appropriate 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 law (see, by way of example, art. 615-ter, penal 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.

_____, XX / XX / XXXX

Data Processor

_____

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 adequate security measures, by storing and controlling the processed data 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.

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 [•], according to Italian law, 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 Italian Civil 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 the provisions of Article 3, paragraph 1, letters a) to o) and r) to u) of Italian Presidential Decree DPR 313 of 14 November 2002, 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 to Articles 60 and 61 of the Italian Code of Criminal Procedure (Ed: 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.).

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 ")

Self-certification

Facsimile SUBSTITUTIVE DECLARATION

(Presidential Decree No. 445 of 28 December 2000)

Messrs
[•]

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

with reference to Contract n. ……

as Data Processor, aware of the penal sanctions referred to in Art.76 of Presidential Decree n° 445 dated 28.12.2000 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.

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 is the Company [•] in the person of its pro tempore legal representative (hereafter ENEL);
- 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 the Italian Data Protection Authority, with registered office in Piazza Venezia 11, 00187 Roma; Rome. Tel. (+39) 06.696771, email: garante@gpdp.it;
- 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 Sub Data Processor by the Data Processor

REF. CONTRACT NO._____

Messrs
Company name of the Supplier
……

Re: **APPOINTMENT AS OTHER PROCESSOR FOR PROCESSING PERSONAL DATA (HEREAFTER "SUB DATA 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 "Data Processor").
2. The Data 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 Data Processor, 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 "Sub Data 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 Sub Data Processor undertakes to perform said operations in accordance with the obligations imposed by the GDPR on the Data Processor and the instructions issued by the Data Controller, who will ensure strict compliance with them.
In particular, whereas the Sub Data 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:

a) It must only process personal data according to ENEL instructions, specifying type of data processed and the categories of Data Subjects;

b) It will have to appoint Authorized Persons ("Authorized Persons") to carry out its data processing operations in IT or paper files, including simple data visualization, by using the specific template provided by ENEL. Before starting the activities covered by the Contract or otherwise by the date specifically communicated by ENEL, the Supplier will also send ENEL a statement concerning the list of appointed employees/collaborators as "Authorized Persons" according to the template provided by ENEL ;

c) It must ensure that Authorized Persons comply with GDPR obligations and Enel instructions and maintain integrity and confidentiality of the personal data during the execution of the Contract and do not to communicate them to third parties, unless expressly authorised to do so by ENEL and except for the cases expressly envisaged by the law; ENEL reserves itself 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) It must adopt all the security measures as set forth in Article 32 of the GDPR, as well as all other preventive measures dictated by the experience designed to ensure the confidentiality and security of the data and minimise the risks that the data in question might be accidentally destroyed or lost or to preclude any processing of data that is not allowed or not compliant with the purposes for which the data are processed; it must also ensure effective collaboration in implementing these measures personal data breaches and in assessing the data protection impact when requested by Enel ;

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

f) It may transfer personal data to a third country or to an international organisation located outside the European Union only in the cases envisaged and under the conditions defined by the GDPR, unless otherly required by 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 conflicting 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 support ENEL in deploying its own appropriate technical and organisational measures, to the extent to which this is possible, in order to let ENEL to fulfil it’s duty to respond data subject's request to exercise their rights;

h) 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 its role as Data Processor;

i) It 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 it should erase also the existing copies, unless the law of the European Union or its member States envisages that personal data have to be stored; proof of accomplished erasure has to be provided to Enel;

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

k) It 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;

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

m) It must cooperate with ENEL by making freely available all necessary information in order to allow Enel compliance with Articles 33 and 34 of the GDPR, including up-to-date and valid certifications;

n) According to Article 30 of the GDPR, it must keep a data record of the processing activities carried out on behalf of ENEL, which must be exhibited upon request of ENEL when subject to legal obligations under articles 33 and 34 of the GDPR.

It is forbidden to the Contractor to process personal data for purposes other than the execution of the Contract. In particular, where it is not necessary for the execution of the Contract, it is forbidden for the Contractor to make, by way of example but not exhaustive, to massively extract personal data, also through the use of "RPA - Robotic Process Automation" (or "automata"), unless previously authorized by the Contractor

The Sub Data Processors must comply with the obligations that this Contract imposes on data processors.

The Sub Data 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 Sub Data 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 Sub Data 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 Sub Data 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 Sub Data 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 Sub Data 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 Sub Data Processor intends to process the Personal Data in countries not deemed adequate by the European Commission, the Processor shall ensure that the Sub Data 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 Processor. Without prejudice to the Sub Data Processor's duties to indemnify ENEL, as already envisaged in the Contract, the Sub Data Processor 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 Sub Data 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 Sub Data Processor and Sub Data 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 Sub Data 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,

Processor

_____

For acceptance

Sub Data Processor

_____

Attachment 5 GDPR

List of Sub-processors

COMPANY	COUNTRY AND ADDRESS	PRODUCT OR SERVICES	TYPE OR CATEGORY OF DATA PROCESSED	PRIVACY SHIELD OR OTHER RELEVANT CERTIFICATIONS

Attachment 6 GDPR

RE. CONTRACT N ._____

Subject: **REQUEST FOR AUTHORIZATION OF APPOINTMENT OF SUB DATA PROCESSOR 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, the Company xxx has been identified
- pursuant to Article 28 of the GDPR, this company must be appointed as a Sub Data Processor

IT IS HEREBY AGREED AS FOLLOWS

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

_____, XX/XX/XXXX

Data Processor

_____

For acceptance

Data Controller

_____

Attachment 7 GDPR

Dear NAME AND SURNAME Person Authorised

_____

REF. CONTRACT NO._____

Re:

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

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, which means any operation, even if only for consultation, relating to personal data stored in IT and/or paper files held by the undersigned Company as Data Processor and/or by the Company [•] as 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 to you in relation to processing personal data.

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 consent collection stage must be preceded by a specific privacy notice and by the release 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 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 appropriate 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 law (see, by way of example, art. 615-ter, penal 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.

_____, XX / XX / XXXX

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 adequate security measures, by storing and controlling the processed data 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 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

<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.

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 [•], according to Italian law, 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 Italian Civil 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 the provisions of Article 3, paragraph 1, letters a) to o) and r) to u) of Italian Presidential Decree DPR 313 of 14 November 2002, 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 to Articles 60 and 61 of the Italian Code of Criminal Procedure (Ed: 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.).

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

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, which means any operation, even if only for consultation, relating to personal data stored in IT and/or paper files held by the undersigned Company as Data Processor and/or by the Company [•] as 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 to you in relation to processing personal data.

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 consent collection stage must be preceded by a specific privacy notice and by the release 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 appropriate 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 law (see, by way of example, art. 615-ter, penal 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.

_____, XX / XX / XXXX

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 adequate security measures, by storing and controlling the processed data 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

<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 [•], according to Italian law, 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 Italian Civil 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 the provisions of Article 3, paragraph 1, letters a) to o) and r) to u) of Italian Presidential Decree DPR 313 of 14 November 2002, 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 to Articles 60 and 61 of the Italian Code of Criminal Procedure (Ed: 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.).

Attachment 8 GDPR

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 DataProcessor

Self-certification

Facsimile **SUBSTITUTIVE DECLARATION**

(Presidential Decree No. 445 of 28 December 2000)

Messrs
[•]

The undersigned (surname) (name)……
born in ..... (.....), on ……
(place) ..... (prov.) .....
resident in ……. (…….) Address ……
n. …….. (place)…….. (province.)……..
domiciled in ..... (.....) in Address .....
n. .....(place)…….. (province)……
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 Data Processor, aware of the penal sanctions referred to in Art.76 of Presidential Decree n° 445 dated 28.12.2000 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.

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 Company [•] in the person of its pro tempore legal representative (hereafter ENEL);
- 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 the Italian Data Protection Authority, with registered office in Piazza Venezia 11, 00187- Rome. Tel. (+39) 06.696771, email: garante@gpdp.it;
- 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)
