Date: **06/01/2025**

ENGIE'S BINDING CORPORATE RULES

This document is the **public version** of the ENGIE's Binding Corporate Rules. It is the result of the complete version, minus the confidential information that cannot be disclosed to the public.

Table of Contents

1 Introduction

ENGIE SA ("ENGIE SA") and the ENGIE entities listed in Appendix A (*not disclosed as confidential*) as amended from time to time (the "ENGIE SA Subsidiaries") (collectively referred to as the "ENGIE Group") shall, in the course of their activities, process Personal Data concerning their employees and other related personnel (such as job applicants, etc.) (the "Data Subjects").

Aware of the importance of Data Protection, the ENGIE Group is committed to protecting the Personal Data of Data Subjects and to ensuring compliance with the Personal Data Protection legislation applicable in the countries where the ENGIE Group operates.

To this end, the ENGIE Group has already established uniform and adequate Data Protection standards for the Processing of Personal Data of Data Subjects, by updating the Group Personal Data Protection Policy (see Appendix B – *disclosed in its public version*) on 29 July 2022.

The purpose of these Binding Corporate Rules ("BCR") is to supplement the Group Personal Data Protection Policy and the Code of ethical conduct in order to ensure an adequate level of protection for transfers and associated Processing of Data Subjects' Personal Data within the ENGIE Group, and to facilitate transfers of Data throughout the Group, in accordance with applicable legal provisions, in particular those set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation, or "GDPR"). Each ENGIE SA Subsidiary will ensure that these BCR and the Group Personal Data Protection Policy are complied with before any Data Processing, during its execution and operation.

Thus, the directors, managers and employees of these Subsidiaries undertake to comply at all times with these BCR when collecting, using, transmitting and Processing Personal Data relating to a Data Subject.

These BCR are communicated to all ENGIE Group employees (in particular via the intranet and by internal memo of the Ethics, Compliance & Privacy Department of the ENGIE Groupe, as well as at the level of each Entity by any other means decided by it) and are available on the ENGIE website at the following address: https://www.engie.com/en/group/ethics-and-compliance.

If you have any questions about these BCR or concerning rights of the data subjects and Third Party Beneficiaries, or for any other questions regarding the Protection of Personal Data, please contact the Group Data Privacy Manager via the contact link or your BU Data Privacy Manager via the group DPO directory.

2 Définitions

For the purposes of these BCR, terms and expressions beginning with a capital letter shall have the meaning ascribed to them below, it being understood that, irrespective of the definitions below,

the terms of these BCR shall in any event be interpreted in accordance with the applicable European legislation, namely at the date of execution of these BCR, the GDPR.

« **Applicable Legislation** » means the national legislation applicable in the country in which the Data Controller is located and from which it transfers Personal Data. Where the Data Controller transfers Data from a Member State of the European Economic Area, the term 'Applicable Legislation' includes Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or "GDPR").

« **Data** » or « **Personal Data** » means any information relating to an identified or identifiable natural person. A natural person shall be deemed identifiable where he/she 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 his or her physical, physiological, genetic, mental, economic, cultural or social identity. The Personal Data subject to these BCR is "HR Data" as defined below.

« **HR Data** » means any Personal Data relating to Data Subjects who are staff members, namely employees, applicants, trainees, temporary workers or retired employees of any ENGIE SA Subsidiary.

« **Data Controller** » or « **Controller** » means the natural or legal person, public authority, department or other body that determines, alone or jointly with others, the purposes and means of the Processing of Personal Data.

« **Data Exporter** » or « **Exporter** » means the Controller established in the EEA that transfers Personal Data.

« **Data Importer** » or « **Importer** » means, if the context so requires: (i) the Data Controller who agrees to receive from the Data Exporter personal data for further Processing in accordance with the terms of these BCR or (ii) the Data Processor who agrees to receive from the Data Exporter personal data to be Processed on behalf of the Data Exporter - after transfer - in accordance with its instructions and the terms of these BCR.

« **Data Privacy Manager** » (« **DPM** ») means the person designated as responsible for the actions related to the Protection of Personal Data at the level of a Regional Hub or a Subsidiary. When he or she takes up his or her position, he or she receives a letter of assignment from his or her superiors.

« **Data Processing** », « **Processing** » or « **Processing** » means any operation or set of operations, whether manual and/or automated, carried out or not by means of automatic processes, on Personal Data, such as collection, recording, organisation, storage, adaptation or

modification, retrieval, consultation, use, communication by transmission, dissemination or any other form of making available or transfer, reconciliation or interconnection, limitation, deletion or suppression. The Data Processing and its purposes that fall within the scope of these BCR are further defined in Appendix C.

« **Data Protection Authority** » means an independent national authority responsible for, among other things, verifying compliance with the Data Protection laws applicable in its country. A list of Data Protection Authorities is available on the web page https://edpb.europa.eu/about-edpb/board/members_en

« **Data Protection Committee** » (« **Privacy Committee** ») means the Committee created under the ENGIE Group Personal Data Protection Policy, whose objective is to carry out activities aimed at promoting and/or ensuring the application of the ENGIE Group Personal Data Protection Policy.

« **Data Protection** » or « **Personal Data Protection** » means all measures, activities, methods, processes, organisations, etc. aimed at protecting Personal Data and ensuring compliance with applicable laws and regulations on Personal Data Protection.

« **Data Protection Officer** » (« **DPO** ») means the person who is officially appointed to the competent Data Protection Authority in accordance with the GDPR. The Data Protection Officer may simultaneously be the Data Privacy Manager of a Regional Hub or a Subsidiary.

« **Data Processor** » or « **Processor** » means the natural or legal person, public authority, department or any other body that processes Personal Data on behalf of the Data Controller.

« **Data Subject** » means an identified or identifiable individual whose Personal Data is being Processed, regardless of nationality. (defined as members of the personnel, i.e. employees, consultants, applicants, interns, temporary workers or retired employees of any Subsidiary of ENGIE SA)

« **EEA** » means the European Economic Area.

« **ENGIE Group** » means ENGIE SA and all the Subsidiaries/Entities of ENGIE SA.

« **ENGIE Group Personal Data Protection Policy** » means the principles and objectives, and the organisation and monitoring system that have been implemented, as well as the roles and responsibilities with respect to Personal Data Protection, set forth in Appendix B (*disclosed in its public version*).

Global Business Unit (GBU) : means the organization established to carry out business, consisting of several Group Entities grouped by business segment. The GBUs do not have a Data Privacy Manager (DPM) but a General Counsel who works with the DPMs or DPOs of the Subsidiaries and Regional Hubs.

« **Group Data Privacy Manager** » means the person appointed within ENGIE SA, responsible for Personal Data Protection at the level of the ENGIE Group, in order to define and transmit the good practices relating to Personal Data Protection, and to guarantee their implementation. The Group Data Privacy Manager is also the Data Protection Officer (DPO) of ENGIE SA.

« Regional Hub » refers to the teams responsible for supporting the GBUs and Subsidiaries, for pooling support functions at the regional level, in particular by providing coordination in privacy matters.

« **Special categories of personal data** » means any Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as genetic Data, biometric Data for the purpose of uniquely identifying a person, Data concerning health, sex life or sexual orientation. These data will be referred to interchangeably as “Special categories of personal Data” or “Sensitive Data”.

« **Subsidiary(ies) of ENGIE SA** » or «**Subsidiary(ies)** » means the legal entities within the Group's scope of consolidation (full consolidation) as indicated in Appendix A attached hereto in its successive amended versions pursuant to Article 6 below (*not disclosed as confidential*). Each ENGIE Subsidiaries concerned by the scope of the BCRs is considered as a Member of the BCRs. The ENGIE Group's new internal organization also refers to it as a "**Business Entity**".or “**Entity”**.

« **Third Party** » means any natural or legal person who is not a Data Subject, including any public authority, department or body other than ENGIE SA and the Subsidiaries of ENGIE SA.

« **Third party beneficiaries** »: for the purposes of these BCR, the Third Party Beneficiaries are the Data Subjects.

« **Transfer** » refers to any communication, copy or movement of personal data intended to be processed in a country outside the European Union.

3 Scope of the BCR

3.1 These BCR aim to ensure an adequate level of protection and to provide appropriate safeguards throughout the ENGIE Group (see Appendix A for a list of ENGIE Group Subsidiaries subject to BCR – *not disclosed as confidential*), for all categories of Personal Data and for all transfers and associated Processing specified in Appendix C in accordance with the purposes set out in that Appendix.

3.2 These BCR therefore apply to all transfers and Processing of Data Subjects' Personal Data within the ENGIE Group and, more specifically, to all Data Subjects' Personal Data:

- which are processed in the European Economic Area (EEA) by ENGIE SA and/or one of the Subsidiaries of ENGIE SA with its registered office in the EEA;

- which are processed by ENGIE SA and/or one of the Subsidiaries of ENGIE SA with its registered office in the EEA and which are subsequently transferred or made available to one of the Subsidiaries of ENGIE SA with its registered office outside the EEA;

- which are Processed outside the EEA by one of the Subsidiaries of ENGIE SA with its registered office outside the EEA and which are transferred or made available by the recipient of the collection to ENGIE SA and/or one of the Subsidiaries of ENGIE SA with its registered office in the EEA for the purpose of Processing, whether or not this Processing taking place in the EEA involves the onward transfer of the Personal Data to the recipient of the collection whose registered office is outside the EEA.

These BCR do not cover Personal Data processed exclusively outside the EEA. The Processing of Personal Data collected outside the EEA by one of the Subsidiaries of ENGIE SA having its registered office outside the EEA, which are not subsequently transferred to the EEA, in whole or in part, is subject only to the national Data Protection law that is applicable in the country where the Data are Processed.

Without prejudice to the foregoing, these BCRs apply to any Data Subject whose Personal Data is transferred between Entities, the scope of which is not limited to citizens of the European Economic Area.

4 Relationship between BCR and applicable national laws

4.1 Each Exporter and/or Importer of Data in the ENGIE Group must ensure that transfers and Processing of Personal Data of Data Subjects comply with these BCR and, in any case, with the Applicable Legislation. Each Exporter and/or Importer of Data undertakes to provide additional safeguards where the Personal Data includes Sensitive Data, in accordance with article 7(e) below by carrying out a compatibility analysis of the relevant local legislation by means of, among other things, a transfer impact assessment. Under no circumstances may these BCRs be used as a transfer tool without prior analysis of local legislation and without ensuring that the latter does not prevent the correct application of the obligations set forth herein.

4.2 If the Applicable Legislation requires a higher level of Personal Data Protection, the Applicable Legislation will prevail over the BCR. In the opposite case, if the Applicable Legislation provides for a lower level of Personal Data Protection than that provided for in these BCR, the provisions of the BCR shall apply.

The Entities, when assessing the laws and practices of the third country that may affect compliance with the commitments contained in these BCRs, shall take into account :

- The specific circumstances of the transfers or of all transfers, and of any further transfer envisaged within the same third country or to another third country, including the purposes for which the Data is transferred and processed, the types of entities involved in the Processing project, the economic sector in which the transfer takes place, as well as the categories and formats of Personal Data transferred, the place of Processing and storage of the Data and the transmission channels used;

- The laws and practices of the third country of destination relevant to the circumstances of the transfer, including those requiring the disclosure of Data to public authorities or allowing access to such authorities and those providing for access to such Data during transit between the country of the Exporter and that of the Importer;

- The relevant technical and organisational safeguards put in place to complement those provided for in these BCRs, including the measures applied during the transmission and Processing of the Data in the country of destination.

4.3 If an ENGIE SA Subsidiary has reasonable cause to believe that Applicable Law will prevent it from performing its obligations under this BCR and will impair the safeguards provided under this BCR to Data Subjects, it shall immediately notify the Group Data Privacy Manager, unless prohibited by a law enforcement authority. In such cases, the Group Data Privacy Manager will decide on the action to be taken and will in any case inform the CNIL and any other competent Data Protection Authority. When additional guarantees to the measures provided for in these BCRs are to be implemented, the Entities and their Data Privacy Managers are informed and involved in the evaluation and deployment of the measures. The Entities document this assessment. Entities acting as a Data Importer shall promptly notify the Data Exporter where the Data Processing relies on the BCRs as a transfer tool, if they have evidence to suggest that the Data Exporter has become subject to a national regulation or practice that would prevent it from fulfilling its obligations under these BCRs, in particular following a change in legislation. This information is communicated to all Subsidiaries.

4.4 Once notified, the Entity acting as Exporter undertakes to promptly identify additional technical and organizational measures to ensure security and confidentiality to be adopted in order to fulfill its obligations under these BCRs. The same shall apply if an Entity acting as a Data Importer has reason to believe that an Entity acting as a Data Exporter can no longer fulfil its obligations under these BCRs, in accordance with articles 4.4 and 4.5.

4.5 In the event that it is impossible to enforce these BCRs, even with additional measures, the Entity acting as a Data Exporter undertakes to suspend the transfer of Data as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance with these BCRs is re-ensured or the transfer is terminated

The Entity acting as a Data Exporter shall terminate the transfer if the application of the BCRs cannot be reinstated within one month of the suspension. In such cases, Data transferred prior to suspension will be deleted or returned in its entirety. The analysis carried out which made it possible to arrive at the finding that it is impossible to apply the BCRs within this one-month period is shared with all the DPMs of the Entities.

4.6 The Entities acting as Data Exporters ensure continuous monitoring, in collaboration with the Entities acting as Data Importers, in order to monitor legislative and regulatory developments in the third countries to which Data transfers take place and which could affect the compliance of the latter.

5 Binding requests for disclosure of Data by a public authority

In particular, when an ENGIE SA Subsidiary receives a binding request for disclosure of Personal Data from a law enforcement authority or a State security body, it will make every effort to suspend the request and must immediately inform the Group Data Privacy Manager, who will inform the CNIL and the competent Data Protection Authority and provide them with as much information as possible as soon as possible regarding:

- the requested data;
- the requesting organisation;
- the legal basis for disclosure, unless otherwise provided by law, and
- The proposed answer envisaged by the Subsidiary to the public authority concerned.

Without prejudice to the aforementioned obligations in article 4, the Entity acting as a Data Importer shall promptly notify the Data Exporter and, if possible, the Data Subject, if it receives a legally binding request from a public authority under the laws of the destination country or other third country for the disclosure of the Data transferred under these BCRs. This notification includes information about the Data concerned, the number of requests received if there have been several, the type of request and the nature of the requesting authority, as well as the legal basis for this request, the response provided. This principle also applies in the event of a finding by the Entity acting as an Importer if it finds direct access by the same public authority. Consequently:

- If it is prohibited from notifying the Data Exporter or Data Subject, the Data Importer will use its best efforts to obtain a waiver from this prohibition with a view to providing as much information as possible and as soon as possible. This must be documented by the Importer in order to be able to demonstrate them at the request of the Data Exporter ;

5.1 The Data Importer shall provide the Entities acting as Data Exporters, on a regular basis, with any relevant information on the requests received by the public authority, including whether such requests have been contested by the Data Importer and the status of such disputes. If the Data

Importer becomes partially or totally prevented from providing the Data Exporter with the above-mentioned information, it shall inform the Data Exporter as soon as possible ;

- The Data Importer retains the above-mentioned information for as long as the Data is subject to the safeguards provided for in these BCRs and makes it available to the competent Data Protection Authorities in the event of a request ;

- The Data Importer shall examine the legality of the request for disclosure and ensure that it is legally justified and within the limits of the powers granted to the said public authority. If the analysis leads to the conclusion that the request is illegal under the laws of the country concerned as well as the applicable obligations under international law, then the Importer responds unfavorably and may exercise remedies. Under no circumstances shall the Importer disclose the requested Data until it is required to do so under the national rules of the country concerned ;

- The Data Importer shall document its legal analysis and any challenges to the disclosure request and shall make such documentation available to the Data Exporter and the relevant Data Protection Authorities as necessary

If, despite its efforts, the Subsidiary in question is unable to inform the competent Data Protection Authorities, it undertakes to provide the Group Data Privacy Manager, who will report to the CNIL and any other competent Data Protection Authority, on an annual basis, with general information on the requests it has received (for example the number of requests for disclosure, type of Data requested, the requesting authority if possible, etc.)

In any case, each ENGIE Group Subsidiary subject to these BCR undertakes not to transfer Personal Data to any foreign public authority in a massive, disproportionate and undifferentiated manner, or in any other way that would exceed what is necessary in a democratic society.

6 Binding nature of BCR on Subsidiaries and employees

These BCR apply to all ENGIE Group Subsidiaries that have signed the Group Agreement providing for their adherence to the BCR and are binding on each of the said Subsidiaries and their respective employees. Appendix A (*not disclosed as confidential*) lists the Subsidiaries for which BCR approval is required.

To this end, each Subsidiary must guarantee the application of these BCR, complying with the Group's Ethics Charter and, where applicable, the following mechanism(s) which must be implemented in accordance with applicable labour law:

- the internal company rules,
- any provision of the employment contract,
- any other provision to make the BCR applicable to its employees.

Each Subsidiary acting as a Data Controller or internal Processor is responsible for compliance with the BCR and must be able to demonstrate compliance. To this end, each Subsidiary or internal Processor that Processes Personal Data in the EEA or from the EEA must:

- maintain a written record, including in electronic form, of all categories of Processing activities; detailing in particular the processing activities as a Data Controller and as a Data Processor where applicable ;

- For the Entity acting as a data controller, the data controller register must contain and detail the name and contact details of the data controller and, where applicable, the joint data controllers, the data controller's representative and the Data Protection Officer or Data Privacy Manager; the purposes of the processing; a description of the categories of data subjects and categories of personal data; the categories of recipients to whom the personal data have been or will be disclosed; data transfers to a third country of the Relevant Entity, including the identification of that third country and the justification for the application of these BCRs to such transfer; finally, as far as possible, the deadlines for the deletion of the various data concerned and a general description of the technical and organisational security measures planned to guarantee the security of the processing;

- For the Entity acting as an Internal Processor, the internal Processor register must contain and detail the name and contact details of the Processor(s) and each Data Controller on whose behalf the Internal Processor acts as well as the names and contact details of the Controller's representative and the Internal Processor and those of the various Data Protection Officers or Data Privacy Managers; The various transfers of personal data to a third country of the Entity concerned, including the identification of that third country and the justification for the application of these BCRs to such transfer; finally, a general description of the technical and organisational security measures planned to guarantee the security of the processing;

- carry out, if necessary, a Data protection impact assessment for Processing operations that may result in a high risk to the rights and freedoms of Data Subjects. In the event that the impact assessment concludes that there is a high risk to the rights of individuals if the processing is deployed, the Subsidiary acting as a Data Controller should consult the competent supervisory authority;

- implement, both at the time of determining the means of Processing and at the time of Processing itself, appropriate technical and organisational measures in application of the principles of data protection by design and data protection by default.

In addition, each Subsidiary acting as an internal Processor that Processes Personal Data in the EEA or from the EEA must cooperate with the Data Controller in carrying out the above operations and comply with its obligations as described in Appendix E (*not disclosed as confidential*).

Each Entity may incur internal sanctions when it violates these BCRs, fails to implement the recommendations issued after the compliance review carried out by the Data Privacy Managers, or does not cooperate during the compliance audit with respect to the BCRs performed by the Data Privacy Managers. Measures may then be taken by ENGIE S.A. and are set out in article 14 of these BCRs.

7 Principles governing the Processing of Personal Data

To guarantee to Data Subjects an adequate and equivalent level of protection throughout the ENGIE Group, ENGIE SA and the Subsidiaries of ENGIE SA undertake to apply and strictly comply with, and shall ensure that the respective directors, managers and employees apply and strictly comply with, the principles set out below when Processing and transferring Personal Data as defined above and in Appendix C for information purposes.

(a) Lawfulness, fairness and transparency of the Processing

Personal Data must be Processed in a lawful, fair and transparent manner with regard to the Data Subject.

Therefore:

(i) the Data Subject shall receive all information required under the GDPR and applicable national Data Protection legislation with respect to the Processing of his/her Personal Data, as specified in Article 8.1 below;

(ii) where applicable, under the Applicable Data Protection Legislation, the Processing must have been subject to the necessary formalities with the relevant Data Protection Authority; and

(iii) the Processing of Personal Data must be based on one of the following legal grounds:

- the consent (explicit, free, informed and unambiguous) of the Data Subject to the Processing; or
- compliance with a legal obligation to which the Data Controller is subject; or
- the performance of a contract to which the Data Subject is a party or prior to the conclusion of a contract at the request of the Data Subject; or
- the protection of the vital interests of the Data Subject or another individual; or
- the performance of a task in the public interest or in the exercise of a public authority vested in the Data Controller; or

- the fulfilment of the legitimate interest of the Data Controller or of a third party, unless the interests or fundamental individual rights and freedoms of the Data Subject prevail.

(b) Limitation of the purpose of the Processing

Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes, including by Data Importers acting as Data Controllers.

Where Processing for a purpose other than that for which the Data was collected is not based on the consent of the Data Subject or the Applicable Data Protection Legislation, the Data Controller shall determine whether the Processing for another purpose is compatible with the original purpose for which the Personal Data was collected. When the situation arises, the Data Controller carries out a compatibility assessment, the template of which is provided by ENGIE SA and includes the various analysis criteria. The analysis is carried out by the Data Controller and is kept to justify any reuse of data whose purposes are not those of the original purpose. If concerning the original purpose of cross-group data processing, the results of this compatibility assessment is presented to all DPMs of GBU, Hub and entities.

The above-mentioned compatibility assessment will take into account :

- Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing ;
- The context in which the personal data have been collected,
- The nature of the personal data collected, in particular whether special categories of data or whether personal data related to criminal convictions and offences ;
- The possible consequences of the intended further processing for data subjects and the existence of appropriate safeguards.

(c) Minimisation and accuracy of personal data Processed

Personal Data collected, transferred or Processed must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further Processed.

Furthermore, the Personal Data must be accurate and kept up to date, completed and updated. Each Data Controller shall take all reasonable steps to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay.

(d) Limitation of the retention of Personal Data

The period of retention of the Personal Data Processed shall be defined according to the intended purpose of the Processing of the Personal Data. Personal Data must be kept in a form that allows the identification of Data Subjects for no longer than is necessary for the purposes for which it is collected and subsequently processed.

If the personal Data collected are no longer necessary for the purposes of their Processing, such Data must be deleted or made anonymous, in accordance with the Applicable Legislation.

(e) Additional safeguards for Sensitive Data

Sensitive Data shall not be collected, transferred and/or Processed unless such Processing is based on one of the following legal grounds:

(i) the Data Subject has given his/her explicit consent (unless prohibited by Applicable Laws); or

(ii) the Processing is necessary for the purposes of complying with the specific rights and obligations of the Data Controller or the Data Subject in the field of labour law, social security and social protection insofar as this is permitted by the Applicable Legislation with the provision of adequate safeguards; or

(iii) the Processing is necessary for the protection of the vital interests of the Data Subject or of another person, where the Data Subject is physically or legally incapable of giving consent; or

(iv) the Processing relates to Personal Data which are manifestly made public by the Data Subject; or

(v) the Processing is necessary for the establishment, exercise or defence of legal claims ; or

(vi) the Processing is carried out in the course of legitimate activities by a foundation, association or other non-profit organisation whose object is political, philosophical, religious or trade union, subject to appropriate safeguards being provided for that purpose and provided that the Processing relates only to members or persons having regular contact with that organisation and that the Personal Data is not disclosed to a third party without the explicit consent of the Data Subject; or

(vii) the Processing is necessary for important public interest reasons, on the basis of the Applicable Legislation which must be proportionate to the objective pursued, respect

the essence of the right to Data Protection and provide for appropriate and specific measures to safeguard the fundamental rights and interests of the Data Subject; or

(viii) the Processing is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health, or for the purpose of ensuring high standards of quality and safety of health care and medicines or medical devices, on the basis of Applicable Legislation which provides for appropriate and specific measures for the safeguarding of the rights and freedoms of the Data Subject, including professional secrecy; or

(ix) the Processing is necessary for archival purposes in the public interest, for scientific or historical research or for statistical purposes, on the basis of the Applicable Legislation which must be proportionate to the objective pursued, respect the essence of the right to Data Protection and provide for appropriate and specific measures to safeguard the fundamental rights and interests of the Data Subject; or

(x) the Processing of Sensitive Data is necessary for the purposes of preventive or occupational medicine, assessment of the worker's capacity to work, medical diagnosis, health or social care, or the management of health care or social protection systems and services on the basis of Applicable Legislation or by virtue of a contract with a health professional, and must be assumed by a health professional or any other person bound by professional secrecy or subject to an equivalent secrecy obligation by virtue of the law or regulations issued by the competent authorities.

(xi) The Processing of Personal Data relating to criminal convictions and related offences or security measures may only be carried out under the control of the competent Data Protection Authority, or if the Processing is authorised by the European Union law or by the law of the Member State concerned which provides appropriate safeguards for the rights and freedoms of data subjects.

(f) Specific rules applicable to automated individual decisions

An evaluation or decision concerning Data Subjects that either produces legal effects with respect to the Data Subject or significantly affects the Data Subject may in no event be based solely on the automated Processing of their Personal Data (including profiling), unless that decision:

(i) is necessary for the conclusion or performance of a contract between the Data Subject and a Data Controller; or

(ii) is authorised by a law which also lays down appropriate measures for safeguarding the rights and freedoms and legitimate interests of the Data Subject; or

(iii) is based on the explicit consent of the Data Subject.

In the cases referred to in (i) and (iii) above, the Data Subject may: (i) obtain human intervention from the Data Controller, (ii) express his/her point of view and, (iii) if necessary, challenge the decision.

(g) Security and confidentiality obligations

The ENGIE Group must protect the Personal Data of Data Subjects against unauthorised and accidental access, unlawful Processing, involuntary or unlawful disclosure, loss, destruction or damage. Consequently, the ENGIE Group undertakes to implement appropriate protection measures and, in particular, physical, technical and organisational security measures aimed at adequately guaranteeing the security and confidentiality of the Personal Data of the Data Subjects.

These measures depend on the state of the art, the costs of implementation and the nature, scope, context and purposes of the Processing as well as the risks, which vary in likelihood and severity, to the rights and freedoms of the Data Subjects.

The security measures implemented at the level of the ENGIE Group are defined in particular in the security policies and standards relating to the Information Systems set out in Appendix D (*not disclosed as confidential*).

The Controller and the Processor shall each take steps to ensure that any natural person acting under the respective authority of the Data Controller and the Processor, who has access to Personal Data, shall not Process it, except on the instructions of the Data Controller, unless obliged to do so by the applicable law(s).

Security incidents must be managed in accordance with the rules set out in the Group's Personal Data Protection Policy.

(h) Subcontracting

As soon as ENGIE SA or one of the Subsidiaries of ENGIE SA, acting as a Data Controller, designates a Processor for the Processing of Personal Data of Data Subjects, within or outside the scope of the ENGIE Group, the said Subsidiary of ENGIE SA must ensure that, before transferring Personal Data to any Processor the latter provides sufficient guarantees as to the technical and organisational security measures governing the Processing, and must ensure that the selected Processor complies with these measures.

Therefore, the contract to be concluded with the selected Processor shall include a clause similar to the standard clause provided in Appendix E (*not disclosed as confidential*), which stipulates that the Processor shall act only on the documented instructions of the Data

Controller and shall apply the rules for ensuring security and confidentiality that are incumbent on the Processor.

(i) Transfers of Data to a Data Controller or Third Party Processor located outside the EEA

When ENGIE SA or a Subsidiary of ENGIE SA intends to transfer Personal Data to a Data Controller or Third Party Processor that is established in a third country outside the EEA, then this transfer can only take place if the European Commission has recognised that the third country in which the Data Controller or Third Party Processor is located, or a specific territory or sector within that third country, ensures an adequate level of protection and has issued an adequacy decision to that end. In the absence of an adequacy decision, ENGIE SA or the ENGIE SA Subsidiary may only transfer Personal Data to that Controller or Third Party Processor if appropriate safeguards have been implemented, such as standard contractual clauses approved by the European Commission or by a Data Protection Authority, or if the Controller or Third Party Processor has implemented binding corporate rules, a code of conduct or a certification mechanism approved by the Data Protection Authorities, or any other measure legally recognised as guaranteeing an adequate level of protection. In the absence of an adequacy decision or appropriate safeguards, a transfer to a Data Controller or Third Party Processor in a country outside the EEA may only take place if ENGIE SA or the ENGIE SA Subsidiary transferring the Personal Data complies with one of the legal derogations in accordance with the Applicable Legislation.

Personal Data may only be transferred to a Processor or Subcontractor in a country outside the EEA whose applicable data protection laws and practices, including requirements regarding the disclosure of Personal Data or measures allowing access to such Data by public authorities, do not prevent the Data Importer from fulfilling its obligations under the Applicable Legislation.

The Exporter, through an impact assessment prior to the transfer to the country outside the EEA, must verify whether or not contractual, technical or organisational measures or safeguards are relevant to complement the existing safeguards. If these guarantees are necessary, they will have to be implemented.

If no such measure can be found, then the Exporter will not be able to transfer the Data.

If the transfer has already taken place, the Exporter shall suspend the transfer of Data if it considers that no adequate safeguards can be provided for the transfer or if the competent Data Protection Authority so instructs. In this case, the Exporter has the right to terminate the contract.

The Importer shall cooperate with the Exporter in assessing the compatibility of its national legislation with the Applicable Legislation and shall inform the Exporter of any changes in

its national legislation that are incompatible with the Applicable Legislation. In the event of an incompatibility, the Exporter shall define without delay the appropriate measures to be adopted by the Exporter and/or to be adopted by the Importer to remedy the situation.

(j) Data breach notifications

In the event of a Data breach, the breach shall be notified without undue delay to the Entity through its Data Privacy Manager, as well as to the Entity acting as a Data Controller when another Entity acting on behalf of the latter as a processor or joint Data Controller becomes aware of a Data breach.

After analysis of the risk to the rights and freedoms of the persons concerned by the DPM or DPO of the entity concerned by the Data breach, If necessary a notification to the competent supervisory authority is made without delay of the entity concerned by the Data breach. Notification is only made after verification and analysis of the risk to the rights and freedoms of the Data Subjects and may not exceed 72 hours in the event of a risk.

The notification of the competent supervisory authority includes all the elements detailing the data breach. It is produced on the basis of a breach assessment tool made available to the Group by ENGIE SA and contains in particular the facts that led to the breach, the consequences of the breach for the data subjects and the remedial measures to resolve it.

Finally, and in case of a high risk result to the rights and freedoms of the data subjectfs, the Entity acting as data controller should notify without undue delay the data subjects concerned by the data breach, and this notification includes all the elements above-mentioned.

8 Information and rights of the Data Subjects

8.1 Informing the Data Subjects

(a) To ensure that all Data Subjects are informed of the existence and content of these BCR and in addition to the training sessions that will be provided to ENGIE Group employees as set out in Article 10 below, each ENGIE Group Subsidiary undertakes:

(i) to communicate these BCR, including any updated version, to all employees of their Global Business Unit, Hub or Subsidiary in particular through the Intranet and by internal memo, and

(ii) to make these BCR available at least on the ENGIE website at the following address: https://www.engie.com/en/group/ethics-and-compliance.

(b) Information to be provided when Personal Data has been collected directly from the Data Subject:

Each ENGIE Group Subsidiary also undertakes to provide Data Subjects, prior to any Processing of their Personal Data, with any information that may be required under the Applicable Data Protection Legislation and, in any case, at least all of the following information:

(i) the identity of the Data Controller(s) and its representative(s), if any;

(ii) the contact details of the Data Protection Officer of the Data Controller(s), if any;

(iii) the intended purposes of the Processing of Personal Data and the legal basis for the Processing of Personal Data;

(iv) where the Processing of Personal Data is based on the legitimate interests of the Data Controller or a Third Party, the legitimate interests pursued by the Data Controller or the Third Party;

(v) the recipients or categories of recipients of the Personal Data;

(vi) where applicable, the fact that the Data Controller intends to transfer Personal Data to a third country or to an international organisation, as well as the legal basis for such transfer;

(vii) the period of time during which the Personal Data will be retained or, where this is not possible, the criteria used to determine such retention period;

(viii) the existence of the rights of access, rectification and erasure of his/her Personal Data, the right to restriction of Processing relating to the Data Subject, the right to object to Processing and the right to the portability of the Personal Data as specified below;

(ix) where the Processing is based on the consent of the Data Subject, the existence of the right to withdraw consent at any time, without prejudice to the lawfulness of the Processing based on consent carried out prior to the withdrawal of consent;

(x) the right to lodge a complaint with a Data Protection Authority;

(xi) information on whether the requirement to provide Personal Data is of a regulatory or contractual nature or is a condition for entering into a contract and whether the Data Subject is obliged to provide the Personal Data;

(xii) where applicable, the existence of an automated decision, including profiling, and, at least in such cases, relevant information concerning the underlying logic, as well as the significance and the intended consequences of such Processing for the Data Subject.

The obligation to inform the Data Subject does not apply to the extent that the Data Subject already has this information.

(c) Information to be provided when Personal Data has not been collected from the Data Subject:

(i) To the extent that Personal Data has not been collected directly from the Data Subject, the information set out in 8.1(b) above must be provided as well as the following information:

- the categories of Personal Data concerned,
- the source of the Personal Data and, if applicable, a statement indicating whether or not it is derived from publicly available sources.

(ii) This information must be provided to the Data Subject:

- within a reasonable time after obtaining the Personal Data and no later than one month after obtaining it; or
- if the Data is to be used for the purpose of communicating with the Data Subject, at the latest at the time of the first communication to the Data Subject.

(iii) The obligation to inform the Data Subject shall not apply when the Data Subject already has this information, or the information proves impossible or involves disproportionate efforts in this respect, or if obtaining or the disclosure of the Data is expressly authorised by the Applicable Legislation, or if the personal Data must remain confidential by virtue of an obligation of professional secrecy regulated by the Applicable Legislation.

(d) This information may be made available to the Data Subject on the ENGIE website and/or on the website of any relevant ENGIE SA Subsidiary, and/or in the appropriate policies and charters, and/or in the contracts concluded with the Data Subject involved in the Processing of the Data Subject's personal data and/or by any other appropriate means (correspondence, information note, etc.).

8.2 **Rights of the Data Subjects**

Each ENGIE Group Subsidiary recognises the following rights of the Data Subjects:

(a) the right to obtain from the Data Controller confirmation as to whether or not Personal Data relating to them are being Processed and, where they are, access to such Data as well as the right to obtain a copy of their Processed Personal Data without delay (access).The

Subsidiary may charge a reasonable fee based on administrative costs for any additional copies requested by the Data Subject;

(b) the right to obtain as soon as possible the rectification or deletion of their Personal Data, in particular if their Data are incomplete or inaccurate (rectification and deletion);

(c) the right to receive their Personal Data provided to a controller in a structured, commonly used and machine-readable format, and the right to transmit such Data to another controller where technically possible and without the controller to whom the Personal Data have been communicated having any objection (data portability);

(d) the right to obtain the restriction of the Processing under certain legal conditions (restriction of Processing);

(e) the right to object, at any time and for reasons relating to their particular situation, to the Processing of their Personal Data based either on a mission of public interest or relating to the exercise of public authority vested in the Data Controller or on the legitimate interests of the Data Controller or a Third Party. In this case, the Data Controller undertakes not to process the Personal Data any further, unless the Data Controller demonstrates compelling legitimate grounds that override the interests and rights and freedoms of the Data Subject, or for the establishment, exercise or defence of legal claims (objection);

(f) the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or which affects them in a similar significant way (objection to automated individual decisions);

(g) the right to withdraw their consent at any time where the Processing is based on the Data Subject's consent. The withdrawal of consent will not affect the lawfulness of Processing based on consent before its withdrawal ; and

(h) The right to be notified at each stage until the conclusion of the examination of an application to exercise the above-mentioned rights

9 Rights of Third Party Beneficiaries

9.1 Each ENGIE Group Subsidiary agrees to grant Third Party Beneficiary rights under these BCR to Data Subjects who have suffered harm as a result of a breach of these BCR. Each ENGIE Group Subsidiary therefore acknowledges and agrees that Data Subjects are entitled to exercise their rights under this BCR and to exercise their rights with the relevant Data Protection Authority or court in accordance with Article 9.3 below. Only Data Subjects whose Personal Data are processed in the EEA and/or transferred to a Subsidiary of ENGIE SA in a country outside the EEA under these BCR may exercise these rights.

9.2 The principles that Third Party Beneficiaries can enforce are as follows:

- Lawfulness, fairness, transparency of Processing and purpose limitation of Processing (see Articles 7(a) and 7(b) above);

- Minimisation and accuracy of Personal Data Processed and limitation of Data retention (see Articles 7(c) and 7(d) above);

- Additional safeguards applicable to Sensitive Data (see Article 7(e) above);

- Specific rules applicable to automated individual decisions (see Article 7(i) above);

- Security and confidentiality obligations (see Article 7(g) above);

- Specific rules applicable to sub processing or transfers of Data to a Data Controller or Third Party Processor located outside the EEA (see Articles 7(h) and 7(i) above);

- Transparency and ease of access to BCR (see Article 8.1(a) of BCR);

- Rights of access, rectification, erasure, portability of Data and restriction and right to object to the Processing, notification at each stage or closure of the examination of a request to exercise these rights and to not to be subject to a decision based exclusively on automated Processing and withdrawal of consent (see Article 8.2) ;

- Rules in case national legislation prevents the application of BCR (see Article 4) ;

- Right to complain through the internal complaint mechanism (see Article 12) ;

- Obligation to cooperate with Data Protection Authorities (see Articles 11.2(a)(v) ; 11.2(b)(iv) ; 11.2(c) and 5) ;

- Rights of redress and judicial remedy (see Article 9.3) ;

- The right to bring a class action and to be represented, if necessary before the competent courts, by a non-profit association or any organisation competent for the above-mentioned action ;

- Right of third party beneficiaries to assert their rights as listed in Article 9.2 ;

- The right of Third-Party Beneficiaries to be informed of any further developments in these Binding Corporate Rules by means of a publication of the most recent version of these Binding Corporate Rules as of their validation

    - Each Data Exporter (namely ENGIE SA and each ENGIE SA Subsidiary in the EEA that transfers Personal Data outside the EEA on the basis of the BCR) is liable for any breach of the BCR committed

by an ENGIE SA Subsidiary established outside the EEA that receives the Data (Data Importer).

9.3 Each Data Exporter (namely ENGIE SA and each Subsidiary in the EEA that transfers

Personal Data outside the EEA on the basis of the BCR) is liable for any breach of the BCR committed by an ENGIE SA Subsidiary established outside the EEA that receives the Data (Data Importer). In this case, when a Data Subject considers that his/her rights have not been respected due to a breach of these BCR, he/she may exercise the following rights:

- the right to lodge a complaint with the Data Exporter in accordance with the procedure described in Article 12;
- the right to lodge a complaint with the competent Data Protection Authority, namely the Data Protection Authority of the Member State in which he/she is habitually resident, works or where the breach is alleged to have occurred;
- the right to an effective judicial remedy if he/she considers that his rights under these BCR have been violated as a result of non-compliance with these BCR. In this case, the Data Subject may bring a legal action against the Data Exporter before the courts of the Member State in which the Data Exporter has its place of business or in which the Data Subject has his/her habitual residence;
- the right to bring a class action and to be represented, if necessary before the competent courts, by a non-profit association or any organisation competent for the above-mentioned action .
- the right to obtain compensation from the Data Exporter for the damage suffered and the right to compensation if the Data Subject considers that he/she has suffered material or non-material damage as a result of a breach of the BCR by the Data Exporter.

9.4 Each ENGIE Group Subsidiary cooperates with the competent supervisory authorities in order to demonstrate the respect and implementation of the rights granted to third-party beneficiaries;

9.5 Each Subsidiary of the ENGIE Group shall make every effort to ensure that all of the above-mentioned rights for the benefit of third-party beneficiaries are covered in the legal acts and other contracts entered into by each Subsidiary pursuant to these BCRs.

10 Training

10.1 All personnel within the ENGIE Group and, in particular, employees who have access to Personal Data on a permanent or regular basis, or who are involved in the collection of Personal Data, in the development or acquisition of tools used to process the Data, must be formally informed of

the content of these BCR and, more generally, of the subjects covered, namely legal and security issues.

10.2 Global awareness campaigns and appropriate training sessions (on site or through webinars) are conducted by ENGIE SA at the level of the ENGIE Group. Local actions will also be carried out by the ENGIE SA subsidiaries in addition to these campaigns and training sessions. Thus, all staff within the ENGIE Group will have to undergo training on Data Protection (including on the ENGIE Group's BCR):

(a) as part of their initial training;

(b) as part of regular training at least once every two years;

(c) as required to keep abreast of changes in the law; and

(d) as required, to address any compliance issues that arise from time to time.

10.3 Some staff members will receive additional specialised training, in particular those staff members who work in the areas of HR, IT, Legal [etc.] or whose professional activities include the Processing of Sensitive Data. Specialised training will be provided in the form of modules that complement the basic training and will be tailored to the needs of the course participants.

10.4 Specific training session of the Data Privacy Managers (DPM) is carried out according to the same principles.

10.5 The Data Protection training provided to ENGIE Group staff will cover the following aspects:

(a) What is the Data Protection legislation?

(b) What are the key terminology and concepts in Data Protection?

(c) What are the Data Protection principles?

(d) How does the Data Protection legislation affect the ENGIE Group internationally?

(e) What are ENGIE's BCR?

(f) An explanation of BCR

(g) The scope of the BCR

(h) BCR requirements

(i) Practical examples of how and when BCR apply

(j) The rights that BCR confer on Data Subjects

(k) The impact of the Processing of Personal Data on the privacy of Data Subjects

10.6 To the extent it is relevant to a staff member's assignment, training will cover the following procedures under the BCR:

(a) Procedure on the rights of the Data Subjects

(b) Procedure for updating the BCR

(c) Cooperation procedure

(d) Complaints management procedure

(e) Procedure for handling requests for access to Data by public authorities

10.7 All these actions, at Group or BU level, must be coordinated by the Group Data Privacy Manager and the BU Data Privacy Manager(s) ;

10.8 Training on the application of the BCRs takes place annually, with two training sessions per year. These training courses include the procedures for requesting access to personal data by public authorities. The training materials are updated regularly before each new update of these BCRs.

11 Monitoring the application of BCR

Paragraph not disclosed as confidential

12 Procedure for claims management

12.1 Complaint made to the Data Controller

If a Data Subject makes a complaint about the Processing of his/her Personal Data under the BCR, or if a Data Subject has reasonable grounds to suspect that his/her Personal Data is being Processed in violation of these BCR or unlawfully under Applicable Law, he/she may refer the matter to the DPM of his/her Subsidiary or, if the Subsidiary does not have a DPM, to the DPM of his/her Business Unit.

Claims should be submitted by e-mail and copied to the appropriate DMP.

Applicants or retired employees to whom these BCR apply should send their claims by e-mail to dpo@engie.com or via the contact link or by sending a postal letter to the following address : DPO, ENGIE SA, 1 Place Samuel de Champlain, FR 92930 Paris La Défense, CEDEX 17

The relevant Data Privacy Manager will act as follows:

(i) he or she will inform the Group Data Privacy Manager;

(ii) he or she will trigger an

(iii) investigation; and

(iv) where appropriate, he or she will notify the larger Subsidiaries of the appropriate measures to ensure compliance and monitoring of the procedure until its completion, including measures to facilitate compliance with the procedure.

The Data Subject may lodge any complaint with the competent data protection Authority independently of an internal complaint within the ENGIE Group as referred to above.

12.2 Response to the Data Subject

Within one month of receiving the complaint or request, the Data Privacy Manager of the Data Subject's Subsidiary or the DPM of the Business Unit will notify the Data Subject in writing of ENGIE's position on the complaint and any measures taken or to be taken by ENGIE to remedy the damage. If the Data Privacy Manager concerned is unable to notify ENGIE's position within one month, given the complexity and number of requests, he/she will inform the Data Subject of the date on which ENGIE's position will be notified to him or her. This date shall not exceed three months following receipt of the complaint. The relevant Data Privacy Manager sends a copy of the complaint and its written response to the Group Data Privacy Manager.

12.3 Judicial remedy of the Data Subject

If the Data Subject's complaint is rejected and the Data Subject is not satisfied with the manner in which the complaint was handled, the Data Subject may exercise the rights conferred upon him or her under Article - of these BCR, including the right to make a complaint to the relevant Data Protection Authority and/or to bring an action in a court of competent jurisdiction to enforce his/her rights under the BCR.

At any time, the Data Subject retains the right to lodge a complaint directly with the competent Data Protection Authority and/or before a competent court, without following the internal complaint procedure described in the previous paragraphs.

12.4 Common rules

Paragraph not disclosed as confidential

13 Responsibility

Paragraph not disclosed as confidential

14 Internal measures

Paragraph not disclosed as confidential

15 Cooperation with Data Protection Authorities

The ENGIE Group undertakes to cooperate and to ensure that all members of the ENGIE Group cooperate with the Data Protection Authorities, in particular in the context of audits or investigations by these Authorities, and to take into consideration the advice and recommendations of the Data Protection Authorities concerning any problems relating to these BCR.

This cooperation will include in particular the following actions:

- provide the necessary staff to ensure dialogue with the competent Data Protection Authority;
- thoroughly review and take into consideration decisions mde by any Data Protection Authority having jurisdiction to rule on legal issues relating to Data Protection that may impact these BCR ;
- Provide, upon request, any information on the processing covered by these BCRs ;
- assist in any audit or investigation on the Subsidiary's premises or remotely by a Data Protection Authority as set out in **Erreur ! Source du renvoi introuvable.**(c) above;
- undertake to comply with any official decision of a Data Protection Authority having jurisdiction to rule on any question relating to the interpretation or application of these BCR.

Any dispute related to the exercise of control of compliance with the BCRs by the Data Protection Authorities will be brought and resolved by the courts of the Member State of the Authority concerned, in accordance with the national law of that State. The Entities agree to submit to the jurisdiction of such courts.

These BCRs may in no way be interpreted as a limitation in the cooperation with the Data Protection Authorities concerned in the exercise of their prerogatives, in particular with regard to control.

16 Updating the BCR

16.1 Only the Data Protection Committee can decide on any modification of these BCR.

16.2 The Data Protection Committee shall appoint a team or person to update the list of ENGIE SA Subsidiaries attached hereto as Appendix A (*not disclosed as confidential*).

16.3 ENGIE SA will notify all ENGIE SA Subsidiaries and the relevant Data Protection Authorities as soon as possible of any changes to these BCR and/or to the list of ENGIE SA Subsidiaries, through the relevant Data Protection Authority, provided that:

(a) some of these changes may require a new approval from the competent Data Protection Authority;

(b) any change that may affect the level of protection offered by the BCR or that may significantly impact the BCR, shall be promptly communicated to the Data Protection Authorities, through the competent Data Protection Authority.

(c) updates to the BCR or the list of ENGIE SA Subsidiaries may be made without requesting approval provided that:

(A) the list of Subsidiaries subject to BCR is updated regularly and that the follow-up and recording of BCR updates are carried out, and that the necessary information is provided to the Data Subjects or to the Data Protection Authorities upon their request;

(B) no transfer is made to a newly set-up Subsidiary of ENGIE SA or to a Subsidiary of ENGIE SA that has not yet adhered to the BCR, until such Subsidiary of ENGIE SA is expressly bound by the BCR and is able to comply with them; and

(C) changes to the BCR or the list of ENGIE SA Subsidiaries are communicated once a year to the relevant Data Protection Authorities, through the competent Data Protection Authority, with a concise explanation of the reasons for the update.

16.4 These BCR will specify the date on which the last revision of the BCR took place, as well as the date of the changes.

16.5 ENGIE SA, as the parent company of the ENGIE Group, ensures the updating of the list of entities subject to the BCRs and the Group DPM team ensures the follow-up of the signatures of the group agreements as well as the answers to any questions concerning the deployment of the BCRs. The Data Privacy Managers on their competent scopes (GBU or Hub or entity) also monitor the deployment of BCRs.

17 Contractual documents

The contract documents are listed below in descending order of priority:

1. These BCR;
2. The Appendices to this BCR;
3. The Group Agreement on the acceptance of the ENGIE Binding Corporate Rules signed by each subsidiary of the ENGIE Group.

This order of priority applies and the BCR will always prevail in case of conflict or contradiction.

18 Applicable law

These BCR are governed by French law.

19 Provision of BCR

These BCRs are made available to data subjects as soon as they are published, through various communication channels accessible to the data subjects. These resources are reviewed annually by each DPM on their respective perimeter.

20 Effective Date - Duration and Return

The present BCR will take effect upon signature of the Group Agreement on the acceptance of the ENGIE Binding Corporate Rules.

These BCR shall automatically cease to apply to the signatory Subsidiary:

- without notice, on the date the Group Entity ceases to be a Group Subsidiary;
- after a period of 15 days, following a written notice sent to ENGIE SA by the Group Entity, notifying its decision to terminate this agreement. For the purposes hereof, such termination shall apply only to such Group Entity. The Group Entity will then have to stop Processing the Personal Data that was protected by the BCR.

As of this date, the Subsidiary shall return to ENGIE SA, within an appropriate period of time that may not exceed 1 (one) month, all of the Personal Data that it may have had to Process, in any form whatsoever, within the framework of these BCR.

The Personal Data will be returned to ENGIE SA in the same format as that used by ENGIE SA to make the Personal Data available to the Subsidiary or, failing that, in a format indicated by ENGIE SA. This return will be recorded in a report.

Once the return has been made, the Subsidiary will destroy the copies of the Personal Data held in its systems and must provide proof of this to ENGIE SA at the same time as the return report is signed.

Appendix A : List the Subsidiaries for which BCR approval is required

Not disclosed as confidential

Appendix B: ENGIE Group Data Privacy Policy

The public version of the Group Data Privacy Policy is available on engie.com via the following link: Group Data Privacy Policy | ENGIE

Appendix C: Data Processing & Scope of the BCRs

This appendix sets out the fields and purposes of data processing, the natural persons and the categories of Data covered by the BCRs.

The BCRs apply to all Personal Data of the Group's human resources that are or have been subject to the GDPR and, more specifically, to all Personal Data of employees, consultants, applicants, interns, temporary workers or retired employees of the Group, which have been collected in the EEA, transferred and processed within the Group for the management of its human resources at an international level in the context of its activity. This includes Data in the following areas:

- Organization (directories, organizational charts, as well as controlling access to the Group's IT Systems for traceability or system monitoring purposes, …),
- Compensation and benefits (annual increases, flexible pay, gross salary, share holding, …),
- Recruitment and national / international mobility,
- Human resources development (skills, training, performance assessment, development plans, …) ,
- Staff administrative management (personal data management, payroll, time management, travel allowance/expenses, …),
- Whistle blowing (ethics events, discrimination, …),
- Health, safety and environment (travel safety, personal accidents, …)
- Security incident management (forensics, …),

In all of the above-mentioned areas and relating exclusively to employees, consultants, applicants, interns, temporary workers or retired employees of the Group, the categories of data concerned are as follows:

- Identity data: surname, first name, photograph, gender, date and place of birth, nationality, professional contact details, personal contact details, passport or national identity card references of the country concerned, family situation, marital status, dependent children, type of driving licence;
- Data relating to the professional situation: place of work, internal identification number (GID), date of entry into the Group, seniority, job held and hierarchical position, nature of the contract, disability rate, recognition of the status of disabled worker, other categories

of beneficiaries of various social statuses, opinions and professional surveys during the Group's annual satisfaction surveys;

- Data relating to the permit equivalent to a work permit: type, serial number and copy of the permit for foreign employees;

- Data relating to the employee's career and professional development: date and conditions of recruitment, date, purpose, reason for changes in the employee's professional situation, career advancement, possible disciplinary sanctions, hierarchical advancement, salary expectations, dates of appraisal interviews, identity of the reporting officer, professional skills acquired, objectives assigned, results, assessments of professional aptitude, observations and wishes expressed by the employee, development forecasts;

- Data relating to training: diplomas, certificates, attestations, foreign languages spoken, follow-up of professional training requests and training periods completed, organisation of training sessions and participation in them, evaluation of knowledge and training followed;

- Data relating to occupational medicine and the management of occupational accidents: contact details of the occupational physician, date of the accident or first medical diagnosis, date of the last day of work, date of resumption, reason for the stoppage, status of the work resumed or not, medical condition of the employee travelling internationally, date of medical examinations, fitness for the job, unfitness for the job, proposals for adapting the workstation;

- Data relating to payroll and remuneration elements: social security number of the country concerned, numbers assigned by any social insurance body, pension or provident fund, family situation, marital status, dependent children, scheme and basis for calculating remuneration, elements determining the allocation of additional remuneration, leave and absences giving rise to deductible or compensable deductions, as well as any deductions legally made by the employer, professional expenses, withholding tax rates, amount of remuneration, days of leave, amounts of any bonuses, amounts relating to profit-sharing and employee shareholding of the ENGIE Group;

- Data relating to the employer's social activity: identity of the employee and beneficiaries, income, benefits, benefits requested, invitations and lists for the organisation of elections to employee representative bodies, preparatory documents, minutes, minutes;

- Data relating to the IT tools made available to the employee: directories, organisation charts, surnames, first names, photograph, function, professional contact details, agendas, dates, places, times of professional meetings, subject, persons present, identification of the personnel concerned, distribution of tasks, individual provision of

equipment, nature of requests and tickets for IT and real estate services within the Group, computer directories to define the application and network access permissions, connection data recorded to ensure the security and proper functioning of applications and networks, address book, individual accounts, virtual private networks, discussions on internal collaborative spaces, IP address, information on the IT equipment used, connection logs, usage history, IT synchronization data, IP address-based tenancy, computer diagnostic data, IDs associated with the office suite used within the Group, business telephone number, connection status, availability status on the work environment;

- Data relating to professional whistleblowing channels: identity, functions and contact details of the whistleblower, of the person involved in the investigation of the alert, facts and information concerning the alert, investigation report, follow-up of the alert, connections to the IT tool used to formulate the alert;

- Any other data relating to the Group's natural persons, employees, consultants, applicants, interns, temporary workers or retired employees, which may be processed in accordance with the areas of processing mentioned above.

Appendix D: Security of ENGIE's Information System

Not disclosed as confidential

Appendix E : Group Agreement on BCRs acceptation for the ENGIE Entity

Not disclosed as confidential

Appendix F : ENGIE data protection clause (data controller to data processor)

Not disclosed as confidential