22 December 2020

DATA PROTECTION POLICY

Organisational Model

Contents

DATA PROTECTION POLICY

Organisational Model

1. Introduction

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, hereinafter the "GDPR") became fully applicable on 25 May 2018.

This organisational model ("Organisational Model") comprises the technical and organisational measures that Falck Renewables S.p.A. (the "Company") implements to guarantee — and be able to demonstrate – compliance with the GDPR of the processing of personal data of natural persons carried out directly or by third parties on its behalf, in order to specify the organisational and process safeguards it has set up to guarantee the actual, effective protection of the personal data for which it is the data controller.

2. Scope of application

This Organisational Model applies to directors, executives, employees, collaborators and consultants of the Company, as well as the data processors, suppliers and all other third parties that carry out operations of processing of personal data on behalf of the Company ("Recipients").

This Organisational Model applies to all direct or indirect subsidiaries of the Company, including (i) the Company, (ii) Vector Cuatro S.L.U. and its direct or indirect subsidiaries, as well as (iii) Falck S.p.A. (collectively, the "Group") subject to application of the GDPR1 which, in line with the principles of autonomy and responsibility specific to each Group company, undertake to endorse and adopt this Organisational Model, defining principles of corporate governance and control regarding the processing of personal data in compliance with this Organisational Model.

Each reference to the Company contained in this Organisational Model shall be understood as referring to each Group company.

3. Definitions

In addition to the definitions provided above, for the purposes of this Organisational Model:

"**filing system**": means any structured set of personal data accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;

"**Supervisory Authority**": means an independent public authority established by a Member State pursuant to Art. 51 of the GDPR (https://edpb.europa.eu/about-edpb/board/members_en);

"**consent to the processing**": means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, either through a statement or a clear affirmative action, indicates consent to the processing of his or her personal data;

"**Data Steward**": means the parties who, identified by the Heads of their Business Units, are appointed to supervise and oversee compliance with the Organisational Model by the Recipients, assist the Company in implementing the Privacy Policies and act as the main contacts for issues concerning the processing of personal data within their

[1] Pursuant to Art. 3 of the GDPR, the GDPR applies (i) to the processing of personal data in the context of the activities of an establishment of a data controller or data processor in the European Union, regardless of whether the processing takes place in the European Union or not, as well as (ii) to the processing of personal data of data subjects who are in the Union, by a data controller or a data processor not established in the European Union, where the processing activities are related to: (a) the offering of goods or services,irrespective of whether a payment of the data subject is required, to such data subjects in the European Union,; or (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union.

business units, as well as serving as contact persons for the data subjects and Recipients;

"**biometric data**": means personal data obtained from a specific technical process, which relate to the physical, physiological or behavioural characteristics of a natural person and which may enable or confirm his/her unequivocal and unambiguous identification, such as facial images or fingerprint data;

"**genetic data**": means personal data related to all the genetic, hereditary or acquired characteristics of a natural person, which provide unambiguous information on his/her physiognomy and health conditions. These may be generated, in particular, from an analysis of a biological sample of the natural person in question;

"**health data** ": means all data relating to the physical or mental health of a natural person, including information regarding medical assistance, which may reveal information on his/her health;

"**personal data**": means any information relating to an identified or identifiable natural person (the "**data subject**"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

"**restriction of processing**": means the marking of stored personal data with the aim of limiting their processing in the future;

"**Privacy Legislation**": means all the legal or regulatory provisions applicable to the protection of personal data, including, but not limited to, the provisions of the GDPR and the national regulations on the protection of personal data, as well as the measures and guidelines laid down the Supervisory Authority;

"**Third Countries**": countries outside the European Economic Area;

"**Privacy Policies**": mean the policies and procedures adopted by the Company in order to govern the various aspects of the processing of personal data, which form an integral and substantive part of this Organisational Model, including, but not limited to, the policies attached to this Organisational Model;

"**Privacy Experts**": the parties designated directly by the Company who, in carrying out their functions and within the limits of their assigned powers, act as contact points for the Data Stewards for issues relating to the processing of personal data and, specifically, issues regarding the Company's compliance with this Organisational Model and the Privacy Legislation;

"**profiling**": means any form of automated processing of personal data consisting in the use of such personal data in order to assess certain personal aspects relating to a natural person, in particular in order to analyse or predict factors regarding professional performance, economic position, health, personal preferences, interests, reliability, behaviour, location or movements of said natural person;

"**pseudonymisation**": means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is stored separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

"**data processor**:" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;

"**third party**": a natural or legal person, public authority, agency or body other than the data subject, data controller, data processor and persons who, under direct authority of the data controller or processor, are authorised to process personal data;

"**data controller**": means 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;

"**processing**": means any operation or set of operations performed upon personal data or 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 other provision, alignment or combination, restriction, erasure or destruction;

"**data breach**": means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Expressions in the singular shall keep the same meaning in the plural, where required by the context.

4. Roles and responsibilities

The Organisational Model implemented by the Company is organised in various levels, by recognising the powers and associated responsibilities of various parties:

the Company is the data controller, and is tasked with determining the purposes and means of processing of the personal data, as well as adopting appropriate technical and organisational measures to guarantee, and be able to demonstrate, that the personal data is being processed in compliance with the Privacy Legislation. In particular, the data controller shall, merely by way of example, adopt privacy by design and privacy by default solutions; update the record of processing activities; prepare the disclosure relating to the processing of personal data; set up all organisational requirements necessary to guarantee that data subjects may exercise their rights; order the adoption of measures imposed by the Supervisory Authority; conduct an impact assessment pursuant to Art. 35 of the GDPR; consult the Supervisory Authority in the cases and according to the methods set out in Art. 36 of the GDPR; sign the agreement set out in Art. 28 of the GDPR with the data processors;

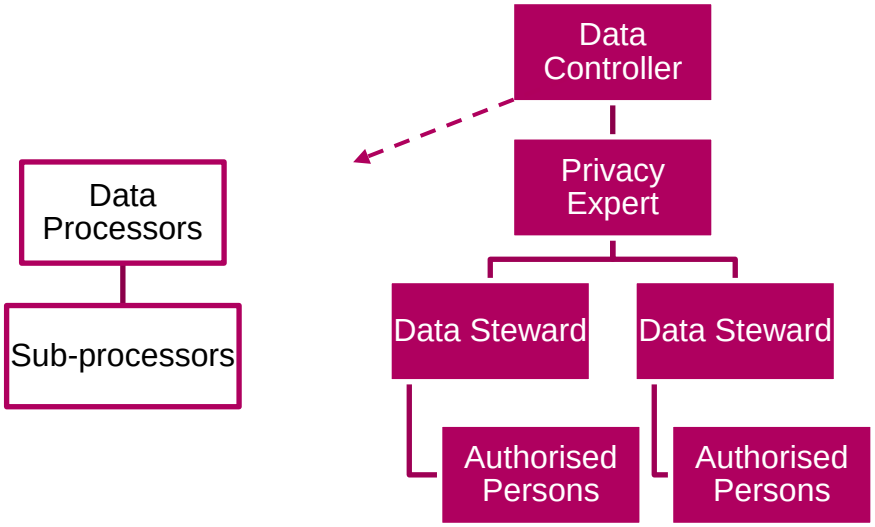
data processors are third parties, outside the Company's organisation, that carry out, on behalf and under the instructions of the data controller, the data processing operations for which the Company is the data controller. Data processors shall sign the agreement pursuant to Art. 28 of the GDPR with the data controller;

sub-processors are third parties, outside the Company's organisation, to whom the data processor assigns the performance of certain processing activities, by entering into a specific agreement which imposes on the sub-processor the same data protection obligations set out in the agreement entered into with the data controller above;

authorised persons are all natural persons that carry out personal data processing operations under instruction from the data controller, including Company employees operating for any reason under the direct authority of the Company;

Privacy Experts are parties identified directly by the Company who, in carrying out their functions and within the limits of the assigned powers, act as a contact point for Data Stewards for issues regarding the processing of personal data and, specifically, issues relating to compliance with this Organisational Model and the Privacy Legislation by the Company. The Privacy Experts can be reached at the e-mail address privacyexpert@falckrenewables.com

“Data Steward”: means the parties who, identified by the Heads of their Business Units, are appointed to supervise and oversee compliance with the Organisational Model by the Recipients, assist the Company in implementing the Privacy Policies and act as the main contacts for issues concerning the processing of personal data within their business units, as well as serving as contact persons for the data subjects and Recipients.



5. Principles applied to the processing

The Company shall carry out processing exclusively in compliance with the principles identified in Art. 5 of the GDPR, pursuant to which personal data shall be:

processed lawfully, fairly and in a transparent manner in relation to the data subject;

collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

accurate and, where necessary, kept up-to-date; every reasonable step must be taken to ensure that data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;

processed in such a way as to guarantee adequate security of personal data, including protection, by means of adequate technical and organisational measures, from unauthorised or unlawful processing and from loss, destruction or accidental damage.

To that end, before processing personal data, Recipients are required to verify compliance with the principles indicated above.

In the event of doubts regarding the correct application of the principles in relation to the specific processing operation, Recipients may contact the Data Steward.

6. Lawfulness of processing;

The Company shall carry out processing exclusively in compliance with the criteria of lawfulness identified in Art. 6 of the GDPR, pursuant to which processing shall be lawful only if and to the extent that at least one of the following conditions applies:

the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

processing is necessary for compliance with a legal obligation to which the data controller is subject;

processing is necessary in order to protect the vital interests of the data subject or another natural person;

processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;

processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

To that end, before processing personal data, Recipients are required to verify that at least one of the requirements of lawfulness indicated above applies.
In the event of doubts regarding the lawfulness of the processing or the legal basis to be used in relation to a specific processing operation, Recipients may contact the Data Steward.

6.1 Consent

Where processing is based on consent, the data controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data. The consent shall be:
freely given (the data subject shall have an actual choice and control over his or her data and must not feel obliged to give consent or suffer negative consequences if he or she does not consent);
specific (must be expressed in relation to one or more specific purposes and the data subject shall be able to make a choice in relation to each of these);
informed (providing information to data subjects before obtaining their consent is crucial for allowing them to make informed decisions, understand what they are consenting to and, for example, exercise their right to revoke consent);
unambiguous (requiring a clear statement or affirmative act from the data subject, which means that consent must always be expressed through a statement or in an active manner. Therefore, silence, inactivity or pre-ticked boxes cannot constitute consent).
The data subject has the right to withdraw his or her consent at any time, and the revocation of consent shall not prejudice the lawfulness of processing based on consent before its revocation. Before granting his or her consent, the data subject shall be informed of this. Consent can be revoked as easily as the way in which it was granted.[2]

In light of the above, before processing personal data based on consent, Recipients are required to verify that the requirements indicated above have been met.
In the event of new processing operations based on consent, the drafting and/or updating of the Company's consent forms is the responsibility of the Privacy Expert, with the support of the Data Stewards and/or the Heads of their Business Units. It should be understood that, having assessed the complexity of the activities requested and after notifying the Company, the Privacy Expert may call upon external consultants to carry out that activity.
It should also be understood that Recipients cannot, under any circumstances, modify or update the Company consent forms without prior written authorisation from the Privacy Expert. In the event of doubts, Recipients may contact the Data Steward.

6.2 Legitimate interest

Legitimate interest is one of the six criteria for the lawful processing of personal data by the data controller. It effectively stipulates that the legitimate interest of the data controller, or of third parties to whom the data is disclosed, shall be assessed in relation to the interests or fundamental rights of the data subject. The result of this comparative test makes it possible to establish whether legitimate interest can be used as the legal basis for

[2] For more details, see also the Guidelines on Consent under Regulation 2016/679 of the Article 29 Working Party.

processing personal data.

To conduct the test, a series of factors must be fully assessed to ensure that the interests and fundamental rights of data subjects are taken into due consideration. At the same time, the comparative test can be adapted, vary from simple to complex, and must not be unduly burdensome. The factors to be considered in executing the comparative test include:

- the nature and origin of the legitimate interest, as well as the possibility that it is necessary to process the data to exercise a fundamental right or otherwise for the performance of a task carried out in the public interest or that it is recognised by the community concerned;
- the impact on the data subjects and their reasonable expectations of what will happen to their data, as well as the nature of the data and the methods of processing;

additional safeguards that could limit the undue impact on the data subject, such as data minimisation, technologies for strengthening the protection of privacy, greater transparency, and the general, unconditional right to revocation and data portability.

In light of the above, Recipients are required to verify, before processing personal data based on legitimate interest, that the data controller has conducted the analysis of legitimate interest illustrated above.

In the event of new processing operations based on legitimate interest, the drafting and/or update of the analysis of legitimate interest of the Company is the responsibility of the Privacy Expert, with the support of the Data Stewards and/or Heads of the specific Business Units. It should be understood that, having assessed the complexity of the activities requested and notifying the Company, the Privacy Expert may call upon external consultants to carry out that activity.

It should also understood be that Recipients cannot, under any circumstances, modify or update the Company analysis of legitimate interest without prior written authorisation from the Privacy Expert. In the event of doubts, Recipients may contact the Data Steward.

7. Transparency

Where personal data relating to a data subject are collected from the data subject, the data controller shall, at the time when said personal data are obtained, provide the data subject with the information set out in Art. 13 of the GDPR. Natural persons should have transparency regarding the methods used to collect, use, consult or otherwise process personal data concerning them, as well as to what extent the personal data are or will be processed. The principle of transparency requires any information and communications relating to the processing of those personal data to be made easily accessible and easy to understand, with the use of clear and plain language.

Before processing personal data, the data controller shall provide the data subjects with the following information:

a) the identity and contact details of the data controller and, where applicable, of the controller's representative;
b) the contact details of the data protection officer, where applicable;
c) the purposes of the processing for which the personal data are intended, as well as the legal basis for the processing;
d) the legitimate interests pursued by the data controller or by a third party, where applicable;
e) the recipients or categories of recipients of personal data, if any;
f) where applicable, the data controller's intention to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or reference to

the appropriate or suitable safeguards and the means for obtaining a copy thereof or where they have been made available.

g) the envisaged period for which personal data will be stored, or, if impossible, the criteria used to determine that period;

h) the existence of the data subject's right to request from the data controller access to and rectification or erasure of the personal data, seek restriction of processing or object to such processing, in addition to the right of data portability;

i) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal, where applicable;

j) the right to lodge a complaint with a Supervisory Authority;

k) whether the provision of personal data is a statutory or contractual obligation, or a necessary requirement for entering into a contract, and whether the data subject is obliged to provide his or her personal data, along with the possible consequences of failure to do so;

l) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic applied, as well as the significance and envisaged consequences of such processing for the data subject.

In light of the above, before processing personal data, Recipients are required to verify that the information above has been correctly provided to the data subjects through the specific disclosure drawn up by the Company. In the event of doubts, Recipients may contact the Data Steward.

In the event of new processing operations, the drafting and/or updating of the Company's disclosure is the responsibility of the Privacy Expert, with the support of the Data Stewards and/or the Heads of the Business Units. It should be understood that, having assessed the complexity of the activities requested and notifying the Company, the Privacy Expert may call upon external consultants to carry out that activity.

It should also be understood that Recipients cannot, under any circumstances, modify or update the Company's disclosure without prior written authorisation from the Privacy Expert.

8. Retention

One of the general principles established by the GDPR is that personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. At the end of that period, the data shall be deleted or anonymised, as no longer necessary for the purposes for which they were collected or otherwise processed.[3]

Mandatory storage obligations may also be imposed by regulatory provisions, including sector-based regulations, or by contractual obligations deriving from agreements with service providers or business partners.

[3] To make specific data anonymous, sufficient elements must be removed to prevent the identification of the data subject. More specifically, the data must be processed in such a way that they can no longer be used to identify a natural person using "*all the means that may reasonably be used*" by the data controller or by others, and the procedure must be irreversible. The most commonly used anonymisation techniques include those based on randomisation, which alter the veracity of the data to remove the strong link between the data and the individual (i.e. if the data are sufficiently uncertain, they can no longer be associated with a specific individual) and those based on generalisation, which 'dilute' the attributes of the data subjects by modifying the respective scale or order of magnitude (meaning a region instead of a town, a month instead of a week).

In order to guarantee compliance with the above principle of limitation of data retention, the Company has drawn up a policy, set out in Attachment E, to illustrate the storage times that shall be applied in processing activities by Recipients.

In light of the above, as part of the processing activities carried out by them, Recipients are required to verify that the above storage times are respected. In the event of doubts, Recipients may contact the Data Steward.

9. Agreement with data processors

Where processing is to be carried out on behalf of the Company, it shall use only data processors that can furnish sufficient guarantees to implement appropriate technical and organisational measures so that processing will meet the requirements of the GDPR and ensure the rights of the data subject are protected.

Furthermore, the Company shall enter into a specific contract with the data processor pursuant to Art. 28 of the GDPR, binding on the data processor with regard to the data controller and that sets out the subject matter governed and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the data controller.

In light of the above, before carrying out processing of personal data that entails the involvement of a data processor, Recipients are required to verify that the Company has signed the above contract with such a processor. In the event of doubts, Recipients may contact the Data Steward.

In the event of new processing operations that entail the involvement of a data processor, the drafting and/or updating of said contract is the responsibility of the Privacy Expert, with the support of the Data Stewards and/or the Heads of their Business Units. It should be understood that, having assessed the complexity of the activities requested and notifying the Company, the Privacy Expert may call upon external consultants to carry out that activity.

The Data Stewards shall keep a complete list of any third parties appointed data processors and, where possible, any sub-processors in their Business Units, as well as notify the Privacy Expert promptly of any updates and/or changes thereto.

The complete list of data processors and, where possible, sub-processors of the Company shall be available from the Privacy Expert.

10. Transfer of personal data to Third Countries

Any transfer of personal data undergoing processing or which are intended for processing after transfer to a third country, including subsequent transfers of personal data by a third country to another third country, shall take place only if the data controller and data processor comply with the conditions set out in Art. 44 et seq. of the GDPR. Specifically, personal data may be transferred only where at least one of the following conditions is met:

a) the third country has receive an adequacy decision from the European Commission;[4]

b) the data controller has furnished appropriate safeguards and provided that enforceable data subject rights and effective legal remedies are available (adequate safeguards comprise, by way of example, binding corporate regulations and standard data protection clauses adopted by the European Commission).

In light of the above, before processing personal data that entails the transfer of personal data to a third country, Recipients are required to verify that at least one of the requirements indicated

[4] The adequacy decisions adopted to this point, in force until modified, replaced or repealed by the European Commission, are listed on the European Commission website (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).

above has been met. In the event of doubts regarding the transfer of personal data to Third Countries, Recipients may contact the Data Steward.

11. The Data Subject's rights

The GDPR allows the data subject to exercise the following rights at any time:

- the right to access the personal data and the following information: purposes of the processing, categories of personal data in question, recipients or categories of recipients to whom the personal data may be communicated, the retention period of the personal data (where possible), as well as, where the personal data is not collected from the data subject, all the information available on their origin;
- the right to rectification of incorrect personal data;
- the right to obtain erasure of personal data concerning him or her:
- the right to request the restriction of processing;
- the right to receive or request the transfer of the personal data concerning him or her in the possession of the data controller in a structured, commonly-used and machine-readable format, for additional personal use or to provide them to another data controller;
- the right to object to processing;
- the right not to be subject to a decision which is based solely on automated processing of his or her personal data, where carried out, which produces legal effects concerning him or her or significantly affects him or her;
- the right to revoke consent, including for purposes connected with the sending of marketing communications (effective only for the future);
- the right to lodge a complaint with a Supervisory Authority.

Restrictions could apply to the above rights where the exercising of such rights could cause actual, concrete harm, for example, to the legitimate interests of the data controller and, despite the fact that these rights may usually be exercised free of charge, the data controller may reserve the right to request a fee for clearly unfounded or excessive requests.

The data controller shall provide the data subject with a response without unjustified delay and, in any event, at the latest within one month from receipt of the request. That deadline may be extended to two months, if necessary, in consideration of the complexity and number of requests. It should be understood that, in the event of extension, the data controller shall inform the data subject of said extension and the reasons for the delay, within one month from receipt of the request.

The Recipients are required to assist the Company so that it can correctly manage requests submitted by data subjects and, in the case of requests from data subjects, to communicate such requests to the Data Steward without delay, who shall communicate them to the Privacy Expert, so that a response may be provided to the data subjects within the mandatory deadlines indicated above.

12. Data Breach

The GDPR requires that, as soon as the data controller becomes aware of a breach of personal data, the controller shall notify the competent supervisory authority of such a breach, without undue delay and, where feasible, no later than 72 hours after having become aware of it, unless the data controller is unable to demonstrate that, in accordance with the principle of accountability, it is unlikely that the personal data breach entails a risk to the rights

and freedoms of natural persons.

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons, such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other economic or social damage to the natural person concerned.

Some examples of personal data breaches which must be promptly communicated to the Data Steward are listed below:

- loss of backups containing personal data;
- access of unauthorised parties to databases;
- attacks on the IT system;
- theft or loss of computers, laptops, portable electronic devices, USB sticks, smartphones/tablets of the Company;
- identity theft and/or *phishing*.

In order to guarantee the correct management of personal data breaches, the limitation of their harmful effects and compliance with the above notification obligations, the Company has drawn up a procedure for managing personal data breaches, set out in Attachment D, to illustrate the methods to be used by the Company to identify the actions necessary to implement in cases where there is an actual or suspected breach of personal data. Said procedure also identifies the parties in charge of assessing the seriousness of the personal data breach.

To that end, in compliance with the stipulations set out in the above procedure, Recipients shall report all potential data breaches of which they become aware by promptly contacting the Data Steward, and assist the Company to correctly manage the personal data breach.

13. Log of processing activities

The data controller shall keep a log of the processing activities carried out under its responsibility. That log shall contain all of the following information, as set out in Art. 30 of the GDPR:

a) The name and contact details of the data controller and, where applicable, the joint data controller, the representative of the data controller and the data protection officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and categories of personal data;
d) the categories of recipients to whom personal data are or shall be communicated, including Third Country and international organisation recipients;
e) where applicable, transfers of personal data to a third country or international organisation, including the identification of the country and the documentation regarding suitable safeguards;
f) where possible, the deadlines established for erasing the various categories of data;
g) where possible, a general description of the measures of technical and organisational security measures implemented.

In light of the above, the Company has implemented the processing log to map the various processing operations of personal data carried out under its responsibility and conduct an accurate risk analysis and processing plan.

The Company tasks the Privacy Expert to update and add to the processing log. At least every six months, the Privacy Expert shall update the record based on the update notifications provided, at least quarterly, by the Data Stewards, with regard to their Business Units.

14. Impact Assessment

Where a type of processing, in particular one which uses new technologies, in consideration of the nature, scope, context and purposes of the processing, is likely to generate a high risk to the rights and freedoms of natural persons, the data controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.[5]

This is one of the most important elements of the new regulatory framework, as it clearly expresses the accountability of the data controller for the processing carried out.

The data protection impact assessment is mandatory in all cases where processing may result in a high risk to the rights and freedoms of natural persons. The cases where a data protection impact assessment may be necessary include the following:

- processing involving assessment or scoring, including profiling;
- automated decisions that generate significant legal effects (e.g. recruitment);
- systematic monitoring (e.g. CCTV surveillance);
- the processing of sensitive, legal or extremely personal data (e.g. information on political views);
- processing of personal data on a large scale;
- combination or comparison of data sets deriving from two or more processing operations carried out for different purposes and/or by separate data controllers, according to methods that exclude initial consent (such as, for example, cases of Big Data);
- data regarding vulnerable persons (children, persons with psychiatric illnesses, asylum seekers or the elderly);
- innovative uses or the application of new technological or organisational solutions (e.g. facial recognition or IoT devices);
- processing which, in and of itself, could prevent the data subjects from exercising a right or availing themselves of a service or a contract.

The impact assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the data controller;
b) an assessment of the necessity and proportionality of the processing operations with respect to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects;
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of data subjects and the other persons concerned.

The data protection impact assessment shall be conducted prior to processing and, in any event, should be

[5] For more details, see also the Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 of the Article 29 Working Party.

continuously re-examined, with the assessment repeated at regular intervals.

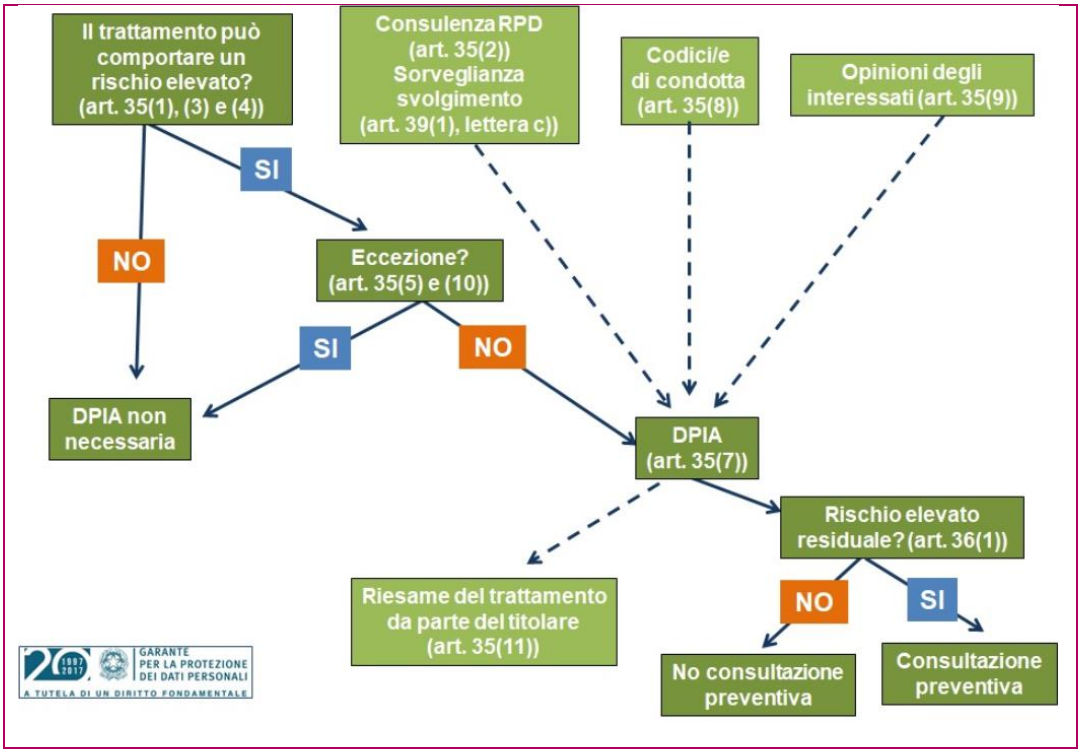
In this sense, the data protection impact assessment allows for concrete compliance of any processing with the data protection by design and data protection by default principles pursuant to Art. 25 of the GDPR. Specifically, in consideration of the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons posed by the processing, the data controller shall, both when determining the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, which are designed to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of the data subjects (privacy-by-design principle).

In the same manner, the data controller shall implement appropriate technical and organisational measures for ensuring that only personal data which are necessary for each specific purpose of the processing are processed by default (privacy-by-default principle).

In light of the above and in order to guarantee the correct execution of the data protection impact assessment, as well as compliance with the above privacy-by-design and privacy-by-default principles, the Company has drawn up the document in Attachment B. This shall be understood as a medium to be tailored to the characteristics of the specific case, for conducting the data protection impact assessment.

The Company has entrusted the Privacy Expert with activities relating to carrying out the data protection impact assessment, including the preventive phase of deciding whether it is necessary to conduct such an assessment, which must be carried out in agreement with the Data Steward and/or the Head of the specific Business Unit, as well as the Recipients concerned. The Privacy Expert must thus be informed by the Data Steward and/or the Head of the specific Business Unit of any new project. The Privacy Expert, in agreement with the company and in consideration of the complexity of the activities required, may call upon external consultants to carry out that activity.

When should the *Data Protection Impact Assessment* (hereinafter, the "DPIA") be conducted?



15. Monitoring and control

In order to verify compliance with this Organisational Model and the Privacy Legislation by the Recipients, including the data processors, the Company shall conduct, at least annually, monitoring and control of the processing carried out by the Company and of the Recipients' compliance with the Organisational Model.

In light of the above, the Company has assigned the monitoring and control activities described above to the Privacy Expert.

After such checks, the Privacy Expert shall send, at least on a yearly basis, to the CEO of the Company and, for information, to Internal Audit, a report indicating, inter alia, any requests from the Supervisory Authority, any potential non-compliance in the processing of personal data and the associated corrective measures, the relevant significant risks or issues in the processing of personal data, a list of data protection impact assessments conducted and/or recommended, new projects and their conformity with the principles of privacy by design and by default.

16. Training

For the Organisational Model to function effectively, the training of Recipients authorised to conduct processing is managed by the Company in close cooperation with the Privacy Expert and the Human Resources Department of the Company. Specifically, training courses cover all the components of the Organisational Model along with concepts relating to Privacy Legislation.

Participation in training courses is monitored through a system or recording attendance. At the end of each training course, participants sit a test to assess their degree of learning and to guide additional training sessions. Participation in training courses is mandatory for all Recipients authorised to conduct processing by the Company. That obligation is a fundamental rule of this Organisational Model, breach of which shall trigger the penalties provided for in the disciplinary system.

Recipients of training shall:

acquire knowledge of the principles and content of the Organisational Model;

understand the operating methods to be used to carry out their work;

actively contribute, in relation to their roles and responsibilities, to the effective implementation of the Organisational Model, reporting any shortcomings detected in the Model.

17. Non-compliance with the Organisational Model

All Recipients are hereby informed that this Organisational Model, as well as the Privacy Policies that form an integral and substantive part thereof, is binding on Recipients.

Any breaches of the Organisational Model, as well as of the Privacy Policies, may have serious repercussions for the Company and, for Recipients that are Company employees, trigger the application of disciplinary measures, in compliance with the legal provisions and the applicable national collective labour agreement, and, for Recipients that are not Company employees, termination of the contractual relationship with the Company, without prejudice to any other actions taken to protect all the Company's rights.

Behaviours that constitute breaches of this Organisational Model may also result in an infringement of legal provisions that could entail civil and criminal consequences for the Recipients.

The Company may also be prosecuted and sanctioned as a result of non-compliant conduct by the Recipients, and a breach of the provisions of the GDPR may result in the application of administrative fines of up to €20,000,000 or up to 4% of the previous year's total annual global turnover, if higher.

18. Updates and amendments

This Organisational Model may be updated, amended or supplemented at any time by the Company. In that case, the amendments shall be brought to the attention of the Recipients in the shortest possible time, through publication in the Company's information channels. To that end, Recipients shall periodically consult the internal communications channels and read the updated version of the Organisational Model.

19. Contacts

In you have any questions or doubts regarding this Organisational Model or the Privacy Policies, please contact the Privacy Expert at the following e-mail address: privacyexpert@falckrenewables.com.

20. List of attachments

A. Policy on the Use of IT Tools (15)
B. Data Protection Impact Assessment(21)
C. F.A.Q. (28)
D. Data Breach Policy (**Errore. Il segnalibro non è definito.**)
E. Data Retention Policy (41)

Attachment A
Policy on the Use of IT tools

1. Scope of application

The purpose of this policy is to define the rules and methods according to which employees, agents and consultants of the Company ("**Users**") may use personal computers, tablets, smartphones, peripherals (including *webcams*, microphones and audio peripherals) and any other IT tool assigned to them or made available by the Company ("**IT tools**") to carry out their duties.

The definitions set out in the Organisational Model apply to this policy. It should be understood that each reference to the Company contained in this policy should be understood as referring to each Group company.

2. Policy on the Use of IT tools

IT tools constitute work tools.

Their use is permitted exclusively for purposes directly pertaining to or in any event connected with work, according to criteria of correctness and professionalism, consistent with the type of work performed and in line with the legal provisions and Company policies, excluding, in any event, any use for private and/or personal purposes.

IT tools are assigned by the Company to Users, with each resulting obligation of appropriate custody and use. Users shall use the IT tools with the utmost care and diligence.

At the date of termination of the contractual relationship with the company, the User shall return the IT tools to the Company.

The use of the IT tools does not result in any ownership, by the authorised User, of the data or information processed using said IT tools, which belong solely to the Company which, therefore, reserves the right, within the limits permitted by the legal provisions, to access such tools using the methods illustrated below.

Any use of the Company's IT tools in violation of this policy, or of any other relevant applicable law, might result in disciplinary sanctions, including dismissal.

3. Obligations

Users shall:

- shut down the IT tools and any peripherals (e.g. personal computers and monitors) when they finish working and in the event of prolonged absence from their workstation, in the absence of further instructions from system administrators;
- adopt the other precautions set out in the procedures and/or instructions provided by the Company, including in the event of short absences;
- have maintenance and/or repairs of IT tools performed only by personnel authorised by the Company;
- avoid any personal use of the IT tools in the workplace or for work use, unless this has been expressly authorised by the Company;
- on a regular basis (at least every three months), clean out the file systems (data folders and e-mail inbox), deleting obsolete or useless files;
- promptly report any anomalies or malfunctions, even partial, of the IT tools, and inform the Company immediately in the event of theft of or damage to such tools;

- comply with any further policies, instructions and/or procedures provided by the Company, relating to the use of the IT tools.

4. Prohibitions

Users shall not:

- install software, even free software (freeware or shareware), on the IT tools that is not distributed and/or, in any event, expressly authorised by the Company, or connect to peripherals. hardware or devices that are not provided by the Company;
- modify the security and confidentiality settings of the operating system, browser software, e-mail software or any other software installed on the IT tools;
- modify or deactivate in any way the screen saver with workstation password function;
- upload or in any case store within the IT tools any computer equipment, data or information that is personal or contains content not relating to the role held;
- upload or in any case computer equipment the content of which (e.g. text, audio or video) is covered by copyright, pertains to or regards confidential data (unless such data must be processed using those means, in accordance with the provisions and instructions, for the duties assigned), makes confidential data accessible, conflicts with rules of law and/or, in any event, concerns leisure or entertainment activities;
- perform activities which reduce the performance of the Company's systems and services, make them unavailable or introduce vulnerabilities or threats to security;

Management of IT tools, including changes to system configurations, may only be carried out by the Company or by parties expressly authorised by the Company. For example, the following are considered modifications to the system and, therefore, cannot be performed except with prior authorisation from the Company:

- modification of existing network connections;
- use of removable devices (e.g. USB sticks, CDs, DVDs, hard disks);
- opening of the housingof IT tools and the modification, elimination or addition of components;
- installation of any software, including that downloaded from the Internet, or of any alterations to the configuration of the IT tools assigned.

the personnel assigned by the Company may, at any time, remove files or applications that they deem to be dangerous for the Company's security, either from IT tools or network drives.

5. Password management

Access to IT tools requires the correct entry of authentication credentials (user name and password).

The following rules have been stipulated for passwords, which:

- must contain at least eight characters, at least one number, at least one capital letter and at least one lower-case letter and at least one special character;
- cannot be a word found in the dictionary, a slang or jargon word in any language, or any one of such words written backwards;
- cannot be based on the User's personal data or that of a family member (e.g. date of birth, address or name);
- cannot be the same as any of the last ten passwords used.

Users shall apply the following security rules when selecting and using passwords:

- passwords cannot be disclosed to other people, even management or system administrators;
- passwords cannot be written down, unless a secure method has been approved by the Company;

- passwords generated by Users cannot be distributed through any channel;
- passwords must be changed if there are indications that the passwords or system may have been compromised (in which case, a security incident must be reported to the Company).

When passwords are assigned or used, the following rules must be followed:

- Users shall keep passwords confidential, and cannot share their username with other Users;
- each User must be able to choose his or her password, where applicable;
- the temporary passwords used when initially logging into the system must be unique and must comply with the above rules;
- the password management system must require that the User change the temporary password on initial sign-in to the system;
- temporary passwords must be communicated to the User in a secure manner, and the User's identity must be verified in advance;
- the password management system shall require that the User select complex passwords;
- the password management system shall require that Users change their passwords every thirty days;
- the password can never be visible on the screen during sign-in;
- if a User enters an incorrect password 10 times in a row, the system shall freeze the account in question.

6. E-mail

6.1 Purposes of use

The Company provides Users with an e-mail service, assigning each User a business e-mail addresses exclusively for work purposes.

The e-mail account provided to Users by the Company is exclusively a work tool. Therefore, the use of the account by Users is permitted solely for purposes directly pertaining to or, in any event, connected with the performance of the duties assigned and the pertinent activities, excluding any use for private and/or personal purposes or reasons.

In order to facilitate the performance of work, the Company may also provide e-mail addresses shared by multiple Users (e.g. e-mail addresses set up for individual Business Units), alongside the individual e-mail addresses.

6.2 Prohibitions

To ensure e-mail is used correctly, it is prohibited:

to use e-mail for personal purposes and, in any event, to send or receive software or IT material or data or information of any type for personal reasons, e.g. to participate in or sign up to debates, online auctions, competitions, forums, social networks or mailing-lists, unless this has been expressly authorised by the Company or is necessary for carrying out work duties;

to send or exchange or save e-mail messages containing sensitive or legal personal data or which could reveal sensitive or legal data (unless this is necessary for carrying out your duties);

to participate in chain e-mails; moreover, should you receive this type of message, you must immediately delete it;

to send or save messages of an offensive, vulgar, defamatory and/or discriminatory nature in relation to gender, race, language, religion ethnic origin, trade union and/or political opinion or membership, infringements of the law, decency or modesty, or, in any event, those that contain offensive content or which could offend or discriminate in any other way, as well as chain messages and/or spam;

to use language or images that are obscene, misleading, defamatory, discriminatory and/or, in any event, could cause damage to the Company or to third parties;

to exchange messages under an assumed name, i.e. impersonating someone other than the actual sender;
to send or receive or exchange e-mail messages, with or without attachments, containing: images, videos or any type of file whose content is illegal, violent and/or pornographic; files subject to copyright (for example music or video files); links to sites with illegal, violent and/or pornographic content; passwords and/or access codes to programmes subject to copyright and/or to internet sites;
to open e-mail messages or attachments with "executable" formats (for example *.exe*) or which link to external content.

6.3 Obligations

Users shall:

- limit the size of messages sent, especially in cases of multiple recipients;
- avoid all conduct that could allow third parties to disclose information of any type attributable to an unaware sender;
- avoid replying to e-mail messages that contain a generic message requesting personal information for reasons not clearly specified (e.g. expiry, loss or technical problems) or which use intimidation (e.g. the threat of blocking your credit card or current account) or, in any event, containing elements that could constitute phishing activities;
- keep their e-mail accounts in order, deleting unnecessary messages and saving in specific sections messages that are important for the Company, keeping the size of such messages and their attachments low, and, therefore, deleting useless or extremely large documents. It should be understood that the destruction of any communication sent or received which has important content or contains contractual or pre-contractual commitments for the Company or contains documents to be considered confidential, insofar as they are marked with the wording "strictly confidential" or similar or, in any event, having such content for other reasons, must be authorised in writing by the Company.

6.4 Absence of the User

In the event of the sudden or extended absence, or due to work requirements that cannot be postponed, the User may:

i. autonomously insert an 'automatic reply' message into the system which advises senders of messages addressed to the User of their absence and suggests contacting another recipient with an e-mail address in the domain @falckrenewablesgroup.com or @vectrorenewables.com;
ii. subject to prior approval in writing from their Data Steward, ask that messages addressed to them be automatically forwarded to another recipient with an e-mail address in the domain @falckrenewablesgroup.com or @vectrorenewables.com;
iii. with approval from their Data Steward, delegate another User (trustee) to check the content of messages and forward to the Company those deemed important for the performance of work. In this case, the e-mail system administrator shall draw up a report of the activity and inform the User of the access made at the earliest opportunity.

Where the User is unable to make the above requests (e.g. when he or she has been admitted to hospital with limited physical-mental abilities), through the system administrator and with prior written approval from the Privacy Expert, the Company shall implement the solution (i) and, where there are specific, justified business continuity reasons that risk being impacted by the sudden, extended absence of the employee, may access the content of the e-mail account. In this case, the e-mail system administrator shall draw up a report of the activity and inform

the User of the access made at the earliest opportunity.

6.5 Signature

Outgoing e-mail shall always contain the following disclaimer on the confidentiality of the communication, in the footer:

"This message may contain information which is confidential or privileged. If you are not the intended recipient, please immediately notify us and destroy this message and any attachments without retaining a copy. Any unauthorized use of this message either whole or partial (including, without limitation, any copying or reproduction on internet websites and any distribution and/or diffusion to third parties) may expose the responsible party to civil and/or criminal penalties. Respect the environment. Do not print this email unless absolutely necessary.

This message may contain information which is confidential or privileged. If you are not the intended recipient, please immediately notify us and destroy this message and any attachments without retaining a copy. Any unauthorized use of all or part of this message (including, but not limited to, any copying or reproduction on internet websites and any distribution and/or diffusion to third parties) may expose the responsible party to civil and/or criminal penalties. Respect the environment. Do not print this e-mail unless absolutely necessary."

7. Internet

Internet access is permitted to Users of the Company solely in order to perform their work activities and always in compliance with internal procedures and applicable laws.

It is strictly prohibited:

- to modify system settings in order to circumvent any safeguards aimed at limiting access to the Internet;
- to establish peer-to-peer connections to the Internet, for any reason;
- to download very large files, so that the network bandwidth available for the systems will not be saturated;
- to download software, even free software (freeware or shareware), that does not meet the Company's standards, in order to avoid unlawful acts and, above all, the serious danger of downloading viruses.

8. Smart-working

Where Users use the IT tools in carrying out their employment relationship, defined by agreement between the Company and the Users, also organised through phases, cycles and goals and without any constraints of time or place ("***smart-working***"), all the rules illustrated in this policy shall apply.

The User must be authorised by the Company to be able to use its IT tools while *smart-working*. In this case, the User shall:

- exclusively use systems and software for which he or she possesses a regular licence and comply with the terms and conditions of use set out by that licence;
- verify that the system used is regularly updated, regarding both the base software and the antivirus and antispam programmes installed;
- verify that the internet (including the *Wi-Fi*) connection used) is password-protected, to guarantee that it is unlikely that unauthorised persons could access the connection;
- guarantee compliance with the rules and principles of security illustrated in this policy.

9. Monitoring and control

For organisational and production reasons, to protect company assets and to verify compliance with applicable laws an regulations, including Company policies, the Company may need to monitor the use of its IT systems and, for example, access e-mails sent or received by the User. This activity however, shall not be regarded as monitoring the activities of the employees and is performed in accordance with the legislative provisions on

workers' rights and the Privacy Legislation.
Controls for the above reasons shall be carried out with respect of the Users' privacy, by company personnel that provide management and support services for company IT services in the capacity of data processor, with the support, where necessary, of the Head of the Business Unit concerned, who shall identify the subject of the search, which may not be indiscriminate, generic or unlimited. No other person will be involved in these activities, nor access the personal data of the Users contained in the company e-mail accounts.
The Company reminds Users that, because the Company's IT systems are equipped with technical systems that log events that occur (i.e. log files), the Company may access that data for the purposes of the aforementioned control. Those logs may be used to search for the source of possible errors or anomalies, but cannot be used to track Users' work.
The Company may need to carry out this monitoring for the following reasons:

- to identify and prevent any unauthorised access to or communication of information;
- to ensure compliance with laws and regulations;
- to prevent, identify or repress criminal activities;
- to check for viruses or other malware;
- in case of suspicion, to investigate or identify inappropriate use of IT tools;
- in case of suspicion, to investigate violations of this policy or other specific Company policies.

Monitoring is carried out within the limits of what is permitted or required by law and as necessary and justifiable for the purposes illustrated above.
Information identified during monitoring (including personal data) can also be used for disciplinary purposes, stored for the duration of each investigative, disciplinary, regulatory or criminal proceeding and disclosed to third parties if necessary or required by law.
Users may contact the Privacy Expert for further information on the scope and type of controls carried out on the Company's IT systems.

10. Use of social media

You are not permitted to access your personal social media accounts, such as Facebook, Twitter or Instagram, using Company IT tools.
It should be understood that the use of your personal accounts on social media, such as Facebook, Twitter, and Instagram, outside working hours and using your own IT tools must ensure no prejudice is caused to the Company (e.g. you may not post confidential documents of the Company). To that end, the Company hereby specifies that:
any use that violates applicable laws and regulations, public order, any rule of decency and/or that could damage the internal and external reputation and image of the Company is strictly prohibited;
only expressly authorised Users shall be allowed to discuss or post on social media anything concerning the Company's products, projects or services;
it is prohibited to share information on the Company's performance, projects, products, services, development prospects, financial data, business agreements, sales figures, strategies or results on social media unless the Users have been expressly authorised to do so;
it is prohibited to discuss or post on social media about third-party competitors of the Company and/or their products or business;
before sharing any content protected by intellectual property rights (e.g. brand names, trademarks, logos),

including rights held by the Company, you must obtain specific, explicit authorisation from the holder of those rights;

data that identify people and their professional relationships (e.g. customers, suppliers, employees or collaborators) cannot be published on social media without the prior, explicit consent of the people involved;

ideas and opinions shall be expressed in a respectful manner appropriate to the context, in order to avoid damaging the dignity of the people and/or businesses concerned.

With regard to the use of professional social media and/or that strictly connected with work (i.e. Linkedin), Users must enter information regarding their position and role held at the Company that is truthful, pertinent and up-to-date.

Users may contact their Data Stewart for additional clarifications on the use of social media.

11. External references

P_STAFF 30 GR – ITGov _ Logical Access Management

P_STAFF 31 GR – ITSec _ Information Security Policy

P_STAFF 27 GR – ITGov _ IT Tools Management Policy

I_STAFF 18 GR – Op. IT Asset Management

Attachment B
Data Protection Impact Assessment

1. Context

1.1 Overview of the processing operation

1.1.1 Which processing operation is being considered?

1.1.2 What responsibilities are connected with the processing?

1.2 Data, processes and support resources

1.2.1 What data is being processed?

1.2.2 What is the life cycle of the data processing (functional description)?

1.2.3 Which resources support the data?

2 Fundamental principles

2.1 Proportionality and necessity

2.1.1 Are the purposes of the processing specific, explicit and legitimate?

2.1.2 What are the legal bases that ensure the lawfulness of the processing?

2.1.3 Are the data collected adequate, pertinent and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)?

2.1.4 Are the data correct and up-to-date?

2.1.5 How long is the data retention period?

2.2 Measures to protect the rights of data subjects

2.2.1 How are data subjects informed of the processing?

2.2.2 How is the consent of the data subjects obtained?

2.2.3 How can the data subjects exercise their rights pursuant to the GDPR?

2.2.4 Are the obligations of the data processors clearly defined and governed by a contract?

2.2.5 In the event data are transferred outside the European Union, do they enjoy equivalent protection?

3 Risks[6]

3.1 Existing or planned measures

No.	Name of control	Description	Controls implemented
	Encryption	The methods implemented to ensure the confidentiality of the data archived (in databases, files, backups, etc.), as well as the procedures for managing the encryption keys (creation, archiving, updating in the event of suspected compromise, etc.) Specify the encryption methods used for the data flows (VPN, TLS, etc.) implemented in processing.	
	Anonymisation	Indicate the methods of anonymisation implemented, the safeguards introduced by these methods against any re-identification, and the purposes for which they are implemented.	
	Partitioning	Methods used for partitioning the processing.	
	Control of logical accesses	Describe how user profiles are defined and assigned. Specify the authentication methods implemented, setting out, where applicable, the rules for passwords (minimum length, required characters, duration of validity, number of attempts before account is frozen, etc.).	
	Traceability	Policies that define the traceability of events and management of related logs.	
	Archiving	Policies for storage and management of electronic file systems containing personal data, for the purpose of protecting, in particular, their legal validity for the entire period necessary (input, storage, migration, accessibility, deletion, archiving policies, protection of confidentiality, etc.).	
	Security of paper documents	Policies relating to paper documents containing personal data used in the processing. Those policies describe how documents are printed out, archived, destroyed and shredded.	

[6] The risk does not refer to the data controller but to the data subject.

	Minimisation of the quantity of data	The following methods can be used: filtering and removal, reduction of identification potential through transformation, reduction of the identifying nature of the data, reduction of the accumulation of data, restriction of access to data.	
	Vulnerabilities	Policies aimed at limiting the likelihood and seriousness of the risks for the resources used during operations (document the operating procedures, inventory, software updates and hardware upgrades, corrections of vulnerabilities, duplication of data, restrictions on physical access to material, etc.).	
	Management of workstations	Measures adopted to reduce the possibility that the characteristics of software (operating systems, company applications, office software, settings, etc.) could be used to damage personal data (updates, physical and access protection, working on a protected network area, integrity controls, *logging*, etc.)	
	Backup	The existence of backup policies that ensure the availability and/or integrity of the personal data, safeguarding its confidentiality (frequency of backups, encryption of data transmission channel, integrity tests, etc.)	
	Maintenance	The existence of a physical maintenance policy for devices, specifying any use of outsourcing. This shall include remote maintenance, where authorised, and specify the methods for managing defective material.	
	Data processing agreements	The personal data communicated to or managed by data processors shall benefit from sufficient safeguards. Exclusively use data processors that provide sufficient guarantees (in particular in terms of expert knowledge, reliability and resources). Demand that the data processor communicate its IT system security policy. Adopt and document measures (security audits, site visits, etc.) to validate the effectiveness of the data protection guarantees offered by the data processor. Those guarantees shall include, in particular: - encryption of the data based on the level of sensitivity or, in the absence of encryption, the existence of procedures that guarantee that the data processor shall not access the data assigned to it - encryption of data transmissions (e.g. HTTPS or VPN	

		connections) - guarantees on network protection, traceability (logs, audits), management of authorisations, authentication, etc. Enter into a contract with the data processors that specifically defines the subject matter, duration, purposes of the processing and obligations of the contracting parties. Verify that the contract contains specific provisions relating to the following: - the data processor's obligations regarding the confidentiality of the personal data assigned to them - minimum requirements for user authentication - clauses on the restriction and/or destruction of the data on expiry of the contract - rules for the management and reporting of any incidents. The latter should require notification to the data controller where a security breach is identified or a security incident occurs. Such notification should be made as quickly as possible where the breach regards personal data.	
	Security of IT channels	Depending on the type of network used for the processing (isolated, private or internet), the data controller shall implement adequate protection systems: firewalls, anti-intrusion measures or other (active or passive) devices that guarantee the security of the network.	
	Control of physical accesses	Existence of a control of physical accesses to the premises that host the processing (zoning, accompanying visitors, assigning badges, locking doors, etc.). Indicate whether alarm procedures are in place in the event of a break-in.	
	Traceability of network activity	Existence of measures implemented to promptly detect incidents relating to personal data and obtain elements that can be used to study them or provide proof as part of investigations (event logging policy, compliance with data protection obligations, etc.)	
	Security of hardware	Existence of measures adopted to reduce the risk that the characteristics of equipment (servers, fixed workstations, laptops, peripherals, communication devices, removable media, etc.) could be used to damage personal data (inventory,	

		compartmentalisation, redundancy, restrictions on access, etc.)	
	Prevention of sources of human and non-human risk	Existence of measures to prevent human or non-human sources of risk, even if unlikely, from causing harm to personal data (dangerous goods, dangerous geographical areas, transfer of data outside the EU, climate phenomena, fire, water damage, internal or external accidents or animals).	
	Privacy protection policy	Existence of an organisation that can guide and verify the protection of personal data within the structure (designation of a DPO, creation of a monitoring body, etc.)	
	Management of privacy protection policies	The data controller shall set up a documentary framework that formalises the objectives and rules to apply in the field of data protection (action plan, periodic review of data protection policies, etc.)	
	Risk management	Existence of a policy that defines the processes to control the risks that the processing entails for the rights and freedoms of the data subjects (log of personal data processing operations, the data processed, the media used, risk assessment, definition of existing or planned measures, etc.)	
	Integration of privacy protection into projects	Existence of procedures describing the methods to take account of the protection of personal data in each new processing operation (certifications, specification of references, risk management for the data subject according to internal methodology or that indicated by the Supervisory Authority, etc.)	
	Management of security incidents and personal data breaches	Existence of an operational organisation to detect and manage events that could influence the freedoms and confidentiality of the data subjects (definition of responsibilities, corrective action plan, classification of breaches, etc.)	
	Staff management	Existence of a plan that sets out awareness-raising measures adopted when an employee is hired, and a procedure describing the measures adopted once the employment relationship with parties that access data is terminated.	
	Supervision of data protection	Existence of measures that provide a global, up-to-date view of the status of data protection and compliance with the GDPR (verification of compliance of processing,	

		objectives and indicators, responsibilities, etc.)	
	Other controls		

3.2 Confidentiality of data (disclosure/access)

3.2.1 What could the main impacts on data subjects be if the risk materialised?[7]

3.2.2 What are the main threats that could make the risk materialise?

3.2.3 What are the sources of risk?

3.2.4 What measures among those identified contribute to mitigating the risk?

3.2.5 How can the seriousness of the risk be estimated, especially in light of the potential impacts and measures planned?

3.2.6 How can the likelihood of the risk be estimated, especially with regard to threats, sources of risk and the measures planned?

3.3 Data integrity (alteration)

3.3.1 What would the main impacts on data subjects be if the risk materialised?

3.3.2 What are the main threats that could result in the risk materialising?

3.3.3 What are the sources of risk?

3.3.4 What measures among those identified contribute to mitigating the risk?

3.3.5 How can the seriousness of the risk be estimated, especially in light of the potential impacts and measures planned?

3.3.6 How can the likelihood of the risk be estimated, especially with regard to threats, sources of risk and the measures planned?

3.4 Data availability (loss/unavailability/destruction)

3.4.1 What could the main impacts on data subjects be if the risk materialised?

3.4.2 What are the main threats that could result in the risk materialising?

3.4.3 What are the sources of risk?

3.4.4 What measures among those identified contribute to mitigating the risk?

3.4.5 How can the seriousness of the risk be estimated, especially in light of the potential impacts and measures planned?

3.4.6 How can the likelihood of the risk be estimated, especially with regard to threats, sources of risk and the measures planned?

3.5 Overview of risks with the corrective measures implemented8

	Data confidentiality	**Data integrity**	**Data availability**
Seriousness			
Probability			
Result			

SERIOUS	Maximum 4	4	8	12	16

[7] For example: identity theft; financial loss; physical or psychological damage; loss of control of the data; other economic or social disadvantages; impossibility to exercise rights, use services or take opportunities; damage to reputation or discrimination.

[8] For more details, see the "Guidelines on Data Protection Impact Assessment (DPIA)" of the Article 29 Working Party.

	Significant 3	3	6	9	12
	Limited 2	2	4	6	8
	Negligible 1	1	2	3	4
Risk level (seriousness by likelihood)		Negligible 1.	Limited 2	Significant 3	Maximum 4
		PROBABILITY			

LEVEL	**NEGLIGIBLE**	**LIMITED**	**SIGNIFICANT**	**MAXIMUM**
	The data subject will be unaffected or may suffer minor inconveniences that can be overcome without difficulty.	The data subject may suffer significant inconveniences that can be overcome with some difficulty.	The data subject may suffer significant consequences, which could be overcome, albeit with real difficulty.	The data subject may suffer significant or irreversible consequences which might be impossible to overcome.

4 Opinion of the data subjects

[●]

5 List of versions

[●]

6 Conclusions

On conclusion of the data protection impact assessment, taking account of the nature, scope of application, context and purposes of the processing and the sources of risk, as well as the technical and organisational measures adopted to mitigate any risk, ensuring the protection of personal data, the seriousness of the risk is [●] and the likelihood of the risk is [●].

Attachment C
F.A.Q.

	Question	Answer
1.	I find wording of the privacy policy and consent form difficult to understand. Can I change it?	No, only the Privacy Expert can amend these documents. You will have to contact the Data Steward of your Business Unit, who will consult with the Privacy Expert.
2.	There are a range of consent forms. Can I replace them with a single form that encompasses everything?	No, consent pursuant to the GDPR must be specific. Therefore, where multiple consents are required, they must be separated. In any case, it is impossible to amend the consent forms without approval from the Privacy Expert.
3.	Can I profile employees or customers?	Profiling activities are possible only with respect to data subjects who have given their consent. In any case, before performing these activities, you must consult the Data Steward of your Business Unit.
4.	I am working on a new product or service which will entail the processing of personal data and I only expect to ask an opinion from the legal department before the launch to save time. Can I do it?	No, the GDPR requires that an assessment of the impact of products/services on the processing of data right from the initial design according to the procedure set out in point 12 of the Data Protection Policy.
5.	I keep a list of 'long-standing' customers in a drawer in my desk. Can I do this?	No, there are specific maximum retention periods for each category of data. You must contact the Data Steward to inform him or her about the data that you retained as the Company must be able to map all personal data held on its behalf.
6.	I am about to enter into a contract with an IT supplier that I trust as we have worked together for years and it is very well known in the market. Can I dispense with the checks on its compliance with the Privacy Legislation?	No, the procedure set out in point 8 of the Data Protection Policy must be completed for every new contract entered into by the Company.
7.	I am working from home during the weekend. Can I send documents to my private e-mail address so I can work using my personal computer?	No, that would prevent the Company from protecting the document from potential access by third parties. It is not permitted to send documents relating to work activities to a private e-mail account and save them on devices that are not provided by the Company.
8.	I have just realised that I left my backpack on the train. It contains a list of customers, including their personal data. What should I do?	You must send an e-mail to the e-mail address databreach@falckrenewables.com as there is a risk of unlawful access to such personal data.
9.	My company computer has been stolen, what should I do?	You must send an e-mail to the e-mail address databreach@falckrenewables.com as there is a risk of unlawful access to such personal data.

Attachment D
Data Breach Policy

The objective of this procedure (the "**Procedure**") is to define the principles, methods of identification, resolution and consequent management flows of the Company in the event of a breach of personal data (**Data Breach**) pursuant to Regulation (EU) 2016/679 and the Privacy Legislation.

1. Information about the document

1.1 **Regulatory references**

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the **"European Privacy Regulation"** or "**GDPR**");
- Guidelines on Data Breach of the Work Group pursuant to Art. 29 of Directive 95/46/EC of 6 February 2018 (hereinafter "Group as per art. 29").

1.2 Circulation

Every Data Steward shall circulate this procedure among all the members of the organisational units subject to his or her coordination, both when first issued and following any updates which may be made after the initial issue.

1.3 Recipients of the procedure

All employees and agents of the Company, on an open-ended or fixed-term contract (hereinafter jointly defined as the "**Recipients**").

1.4 Obligation of knowledge

The obligation of knowledge and observance of the contents of this procedure falls upon the Recipients.

1.5 Rules for approving, updating, archiving and distributing the Procedure

The approval, update and amendment of this procedure shall be approved by the Privacy Committee in the case of relevant updates, in accordance with periodic revisions and any amendments which may be made to the documents of the regulatory corpus indicated above and, in any case, on an annual basis.

2. Definitions

In addition to the terms defined in the Data Protection Policy document and those defined in the GDPR, the meaning of the other terms hereunder is as follows:

Privacy Committee	This means the committee formed by the Privacy Expert, CDT&IO and the Data Steward of the relevant structure.
Data Breach	This means a security incident leading to the accidental or unlawful destruction, loss, amendment, unauthorised disclosure or access to personal data transmitted, kept or in any case processed.
Personal Data	Any information concerning an identified or identifiable natural person (Data Subject). A natural person is considered identifiable if he or she can be directly or indirectly identified, with specific reference to an identifying element such as a name, identification number, data related to location, an online identifying element or to one or more characteristic elements of their physical, physiological, genetic, psychic, economic, cultural or social identity. An item of personal data does not only refer to a natural person (i.e. an individual), but also includes individual firms and freelance professionals, whereas data concerning legal persons (i.e. companies) are not subject to the Privacy Legislation. As regards the e-mail address name.surname@falck.it, this is an item of personal data, whereas the generic address info@falck.it is not considered personal data.
Processing	Any operation or group of operations, completed with or without the use of automated processes and applied to personal data or batches of personal data, such as collection, registration, organisation, structuring, preservation, adaptation or amendment, extraction, consultation, use, communication via transmission, circulation or any other form of provision, comparison or interconnection, limitation, erasure or destruction.
Privacy Expert	The party acting as the main contact for all matters concerning compliance with the privacy law.
CDT&IO	Chief Digital Transformation & Information Officer
Data Subject	The natural person (including individual firms and freelance professionals) directly or indirectly identifiable through the personal data subject to processing.
Authority	Competent Supervisory Authority
Crisis Team	The advisory Committee, coordinated by the *Gatekeeper*, assigned to analysing the crisis event as defined in the *Crisis Communication Management Procedure*.

3. Scope of application of the Procedure

Pursuant to Article 33 of the GDPR, in the event of a Data Breach, the Data Controller shall notify the competent supervisory authority of such a breach without undue delay and, where feasible, no later than 72 hours after having become aware of it, unless it is unlikely that the data breach entails a risk to the rights and freedoms of natural persons. Moreover, pursuant to Article 34 of the GDPR, when the data breach is likely to generate a high level of risk for the rights and freedoms of natural persons, the Data Controller shall notify the data subject of the breach without undue delay. Such notification is not required when:

- the Data Controller has implemented adequate technical and organisational measures to protect the personal data, and such measures have been applied to the data subject to the breach (e.g. encryption);
- the Data Controller has subsequently implemented adequate technical and organisational measures capable of averting the occurrence of a high risk to the rights and freedoms of the Data Subjects;
- communication to the Data Subjects requires disproportionate effort (in this case, the Data Controller shall proceed with a public communication or similar measure of equal efficacy).

This Data Breach procedure, drawn up in compliance with that established under the GDPR, is implemented upon the detection of a data breach, and its purpose is to define which actions must be taken by the entire corporate organisation in the event of a breach of the principles described hereabove. This document also contains a description of the circumstances whereby a need may arise to notify and/or communicate the data breach to the Authority and/or the Data Subject.
Failure to observe the regulations set out in this document could lead to serious penalties.

The objective of this procedure is to:
- identify the procedures and channels for detecting a Data Breach;
- make provision for the adequate and timely involvement of the top management structures with regard to critical data breach events so as to guarantee immediate action in compliance with the applicable regulations;
- allow for the prompt adoption of a solution to be implemented in order to limit or mitigate the impact of the data breach on business activities;
- use “Risk events” data in order to improve risk identification and assessment;
- fulfil the obligations set out by the applicable law, while demonstrating the Company's commitment to adopting risk management practices suited to the processing operations performed to the Authority.

3.1 What is a Data Breach and what does it entail?

In relation to the definition given under Art. 4, paragraph 12 of the GDPR, Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

According to Art. 32, paragraph 1 of the GDPR, the controller and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The Company shall, inter alia:
- ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- restore availability and access to personal data in a timely manner in the event of a physical or technical incident.

Starting with such definitions, three different categories of personal data breach may be identified according to the internationally acknowledged principles of security:
- *Confidentiality breach:* occurs in cases of unauthorised or accidental disclosure or access;

- *Availability breach*: occurs in cases of loss or destruction of data in an accidental and/or unauthorised manner;
- *Integrity breach*: occurs where the event concerns unauthorised or accidental alteration of personal data.

A security breach is thereby understood as an accidental, unauthorised or intentional act leading to the disclosure, access, alteration, destruction or loss of personal data, thereby giving rise to the infringement of one or more information security principles.

Event	Description of the event	Security principle breached
Destruction/erasure of personal data	Irreversible unavailability of personal data processed by the Company The breach can be associated with logical, unauthorised erasure (e.g. data erasure, irreversible loss of security measures applied for data protection) and/or physical destruction (e.g. broken media), where it is impossible to recover the information.	Availability
Loss or theft of personal data	Loss of control of physical storage resources, such as removal, theft or loss of devices or paper documents. A breach cannot exist when it is possible to exclude unauthorised access to the data with reasonable certainty and if the loss of physical memory does not lead to a permanent loss of personal data.	Availability and confidentiality
Alteration or modification of personal data	Unlawful, unauthorised alteration or modification of data, which was not detected or modified within the internal processes, thus leading to erroneous processing or disclosure of personal data. An unlawful alteration can take place during normal processing operations carried out by authorised personnel or in the case of fraudulent modifications executed by unauthorised parties.	Integrity
Disclosure of personal data	Unauthorised or improper disclosure of personal data to third parties (natural or legal persons, groups of parties, the public). A breach cannot exist when it is possible to exclude unauthorised access to the data with reasonable certainty.	Confidentiality
Unlawful or unauthorised access	Access to personal information processed by the Company by unauthorised parties.	Confidentiality

A personal data breach can also prove to constitute a risk of harm to the affected parties and may lead to physical, tangible or intangible damages to the latter. By way of example, such damage may include identity theft, financial losses and economic or social damage.

To this end, the data controller shall notify the Authority of the data breach without undue delay and, where feasible, no later than 72 hours after having become aware of it. This requirement shall only be fulfilled if the breach entails a risk to the rights and freedoms of the Data Subjects and the Data Controller is unable to prove that, in accordance with the principle of awareness, such a risk is unlikely (Art. 33, paragraph 1 GDPR). Where not made within 72 hours, the notification shall be accompanied by reasons for the delay and it should be possible to provide the information in subsequent stages without further undue delay.

Merely by way of example, some examples of events which could generate a Data Breach are shown below .These

may concern personal data stored both in electronic and paper format:

- Theft of hardware containing a personal data file system;
- loss of data;
- interruption of data lines (or telephone lines) preventing Data Subjects from contacting the controller or having access to their data;
- ransomware attack causing all the data to be encrypted. No back-ups are available and the data cannot be recovered;
- communication of Data Subjects' personal data to the wrong recipients (not assigned to carry out processing), including communication to persons who are not authorised to access the personal data (e.g. relatives, friends or, in any case, persons other than the Recipients or parties to whom the personal data must be communicated in order to perform the Company's business);
- breaches of Company websites due to cyber attacks, with resulting extraction of the Data Subjects' personal data;
- any installation of malevolent software or viruses downloaded to devices supplied by the Company capable of generating a loss of availability of personal data, abusive access to personal data or the removal of personal data;
- violation of employees' e-mail accounts;
- identity theft reported by the police ;
- physical security beach: theft or intrusion in the controller's/processor's premises;
- Denial of Service (DoS) attacks which indicate a malfunction due to an IT attack where the of an providing a service tocustomers are deliberately exhausted, for example a website on a web server, until it is no longer able to provide the service to customers that request it;
- Distributed Denial of Service (DDoS) attacks, which means that incoming traffic inundating the victim originates from several different sources;
- unauthorised access to data;
- loss or removal of paper or electronic documents containing personal data, e.g. removal or theft of folder containing the data of customers or employees;

3.2 Structures involved

In order to manage any personal data breaches in the best and most functional manner, the Privacy Committee is responsible for managing and assessing any personal data breaches. The Committee provides specific expertise relevant to the protection of data and security of information and IT systems.

4. The steps for managing a Data Breach

4.1 Detection

The process of analysing and managing a personal data breach begins with reporting an event, anomaly or malfunction with could potentially lead to a personal data breach. The time frame for notifying the Supervisory Authority starts from the moment when it becomes aware of the breach. It is therefore essential, first of all, that the channel activating the report is aware of the presence of personal data within the affected set of information.
A breach cannot therefore be considered certified until the detection stage is officially concluded.

Detection of the breach is the step where the type of personal data breach, category of parties involved and classification of the security incident (confidentiality, unavailability, integrity) must be correctly identified.

It is therefore possible to detect breaches both within the Company and outside of it and arrive at the latter by means of direct reporting by the Data Subject, an employee, the police or the Authority, a supplier and, in particular, by the external processors and other channels such as the media.

5. **Procedure in the event of data breach detected by a party within the Company.**

Every breach detected within the Company shall be promptly reported.

As soon as a breach has been identified, moreover, the Recipient concerned shall immediately — and in any case no later than two hours from awareness or suspicion of the personal data breach — inform the Company by e-mail to the dedicated e-mail address databreach@falckrenewables.com, accompanied by the following information:

- the nature of the personal data breach including, and where feasible;
- the categories and approximate number of individuals whose data was the subject of the Data Breach;
- the categories and approximate number of records of personal data in question; and
- all other information suitable for identifying the data subject to the Data Breach and mitigating the negative consequences thereof.

Within the 24 hours following the report, the Privacy Committee shall organise a meeting supported by specialised professionals in the technical/IT field with regard to the type of breach that has occurred. Such procedure shall then continue according to the processes pursuant to paragraph 5.2 below.

6. **Procedure in the event of data breach detected by a party outside the Company**

If any data processor — such as a service provider, agent, business partner or advisor — detects or suspects a breach of personal data of which the Company is the Data Controller, upon identification of the breach said third party shall immediately and without undue delay, and in any case no later than 24 hours of having become aware of the personal data breach, notify the latter via e-mail to databreach@falckrenewables.com.

Within the 24 hours following the report, the Privacy Committee shall organise a meeting supported by specialised roles in the technical/IT field with regard to the type of breach that has taken place, which may also be attended by a representative of the third party in order to obtain further details regarding the breach and ensure a better definition of the actions to be taken to remedy the personal data breach and mitigate possible negative effects. The procedure shall then continue according to the processes indicated in section 5.2 below. Contracts with third parties shall provide for the appointment of a processor who shall make provision for the procedure indicated in this section 5, along with the cooperation obligations stipulated in the GDPR.

For the entire period of resolution of the incident, the information pertaining thereto and shared among the members of the Privacy Committee will be considered confidential and shall only and exclusively be communicated to the business units and corporate officers concerned.

7. Managing and assessing breaches

Following the occurrence of an incident, the Privacy Committee shall launch the breach management activity, by identifying and implementing the most effective containment and combating strategy aimed at minimising all further consequences by means of adopting specific countermeasures and preventing the situation from getting worse, as well as with a view to promptly restoring the availability of and access to the personal data.

Within the 24 hours following the report, the Privacy Committee shall organise a meeting which all the Operational Structures shall also be invited to attend, as deemed necessary for the purposes of collecting information with regard to the personal data breach (the "Structures"). During that meeting, and the stages in preparation for it, the Structures shall obtain all information relating to the data breach from the interested parties. The purpose of the meeting shall be to:

- define the causes, nature and scope of the Data Breach, the quantity, type and number of Data Subjects to which the personal data subject to the breach refer, collecting any information to be notified to the Authority pursuant to Article 33 with the support of the IT department and the Data Stewards;
- analyse the actions already taken and define the actions to be taken so as to remedy the personal data breach and attenuate any possible negative effects (including any remote erasure of data contained in the electronic device); and
- assess the level of risk related to the breach, as described in section 5.3 below, in order to determine whether notification to the Authority pursuant to Article 33 of the GDPR and a communication to the Data Subjects pursuant to Article 34 of the GDPR are necessary.

Here is a (non-exhaustive) list of the activities envisaged to contain the incident:

- constant monitoring of how the situation develops; monitoring of the level of criticality is a continuous process that affects all the incident management phases since, in the absence of effective countermeasures, a development relating to an incident in progress could deteriorate, requiring the progressive involvement of higher corporate levels.
- Analysis of the damage, status of affected assets and volume of breached data.
- Monitoring of the time used and required resources.
- Containment of the incident, minimising its impacts and preventing further damage by applying countermeasures of an organisational/procedural nature, which must be formalised and duly traced.

- Implementation of the activities necessary to restore the situation to how it was prior to the incident, where possible.

The Privacy Committee verifies a report of a potential personal data breach to determine the actual presence of a risk to the rights and freedoms of the Data Subjects, assessing, at the least:

- information relating to the nature of the incident (when, where, type of security breach, systems and/or devices subject to the breach);
- the categories of affected Data Subjects;
- the volume of affected data;
- the measures adopted or to be adopted to remedy the breach;
- likely risks to the rights and freedoms of the Data Subjects affected by the data breach.
- the processes and tools to resolve the incident.

The Company is deemed capable of acquiring a degree of reasonable certainty about the breach of personal data in the event of:

- concrete information regarding the personal data breach;
- evidence of the loss of confidentiality, integrity and availability of the personal data;
- consequences unquestionably deriving from the security incident for the rights and freedoms of the Data Subjects.

8. Risk level

The definition of risk level shall consider all possible consequences and negative effects that may reasonably affect the Data Subjects.

Based on the instructions of the Working Group pursuant to Article 29 "*Guidelines on personal data breach notification under Regulation 2016/679*", published on 6 February 2018, and in particular of the document prepared by ENISA, "Recommendations for a methodology of the assessment of severity of personal Data Breaches", Working Document, v1.0, December 2013, the assessment shall consider the following elements:

- *The Processing Framework (PF):* this criterion considers the type of personal data affected by the data breach in connection with specific factors of the processing that may aggravate or mitigate the impact on the Data Subject (volume of data subject to breach, specific circumstances of the Company or of the Data Subject, public availability of the data, accuracy of the data). The criterion value ranges from 1 to 4.
- *Ease of Identification (EI):* this criterion considers the possibility of precisely identifying a party based on the data subject to breach, by simultaneously considering more than one type of data relating to the same party. This criterion is used as a corrective value of the processing framework, since the lower the level of identifiability of the individual based on common indicators, the lower the severity of the breach.
- *Breach Circumstances (BC):* the specific circumstances of the breach in connection with the breach category (loss of integrity, confidentiality, availability).

It is possible to classify all events by taking all these elements into consideration. Each of the criteria mentioned above has been assigned a set of values, to be selected in relation to the characteristics of the breach subject to analysis.

The final result is converted into a qualitative range of 4 values (Low, Average, High, Very High). Depending on the risk level obtained, the following is detected:

- the presence or absence of prejudices to the data subjects affected by the breach;
- the need to notify the Authority and/or Data Subjects.

Severity of the data breach — summary table	
LOW	The Data Subjects will not be concerned or may face certain minor inconveniences that they may overcome without difficulty (time spent re-entering the information, inconvenience, annoyance, etc.).
AVERAGE	The Data Subjects may face significant inconveniences that they will be able to overcome even though they may face some difficulties (additional costs, denied access to corporate services, fear, lack of understanding, stress, minor physical discomforts, etc.).
HIGH	The Data Subjects may face significant consequences that they may be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting from banks, damage to property, loss of jobs, court summons, worsening of health, etc.).
VERY HIGH	The individuals may face significant or irreversible consequences that they cannot overcome (financial problems such as significant debts or incapacity to work, long-term psychological or physical disorders, death, etc.).

The metrics and methodologies used make it possible to classify as low all events which, despite possessing the formal characteristics of a data breach, do not prejudice the Data Subjects in any way and for which no communication is deemed necessary, either towards the Authority or towards the Data Subjects.
In general, by analysing the classification of the breaches, it is considered that:

- in case of possible *breach of confidentiality or integrity*, if the personal data subject to breach is not intelligible, has been anonymised or pseudonymised, the impact of the breach may be low and there may be no need for notification to the Authority nor to the Data Subjects;
- in case of a potential *loss of availability*, if there are copies or data backups, the impact of the breach may be low and there may be no need to notify the Authority or the Data Subjects;

Should the Company fail to assess the breach within 48 hours following the report due to lack of accurate information, a *worst case scenario* impact analysis will be conducted so that the Authority may be notified within 72 hours following the detection of the breach.

Should the level of severity of the Data Breach be high or very high, requiring notification to be provided to the Authority pursuant to paragraph 5.4 below, it shall be classified as a crisis event pursuant to the *Crisis Communication Management* Procedure, and the Crisis Team shall be involved as stipulated by said procedure.

9. Notification

As mentioned previously, as soon as the data processor is reasonably certain that the breach may result in a risk for the Data Subjects, it shall notify the Authority about all personal data breaches that may result in a risk for the rights and freedoms of the Data Subjects.

Specifically, said notification shall contain, at least:

- a description of the nature of the personal data breach, including, where possible, the categories and approximate number of Data Subjects concerned, as well as the categories and approximate number of records of the personal data in question;
- the name and contact details of the Data Protection Officer or another contact person that may provide further information;
- a description of the probable consequences of the personal data breach;
- a description of the measures implemented or suggested for implementation to remedy to the personal data breach and, if applicable, to mitigate any negative effects.

Should the information not be available within 72 hours, it may be provided during the following stages without any further unjustified delay, and one of the two options below may be chosen:

- *Notification in stages*: due to the complexity of the breach or the extension of the investigative analysis of the security breach, the data processor may provide, within 72 hours, an initial description of the context of the breach in order to warn the Authority. The missing information will be communicated in subsequent stages through further notifications suitable for providing a complete and exhaustive overview of the personal data breach.
- *Notification with approximate data*: approximation of certain information that may be provided in detail in successive stages (e.g. approximation of the number of natural persons affected by the personal data breach).

Generally, if a notification is not sent within 72 hours, the notification shall enclose the reasons for the delay based on the specific circumstances.
The obligation to notify the Authority and/or the Data Subjects will not apply if the Company proves, pursuant to the accountability principle, that the breach does not entail risks for the rights and freedoms of the Data Subjects.

The identification of the absence of risks for the rights and freedoms of the Data Subjects shall consider:

- the result of the Data Breach assessment;
- all possible current or future consequences arising from the loss of security principles, as well as of the data protection: integrity, availability, confidentiality;
- the technical and organisational measures implemented previously and subsequent to the personal data breach in order to protect the Data Subjects by reducing the impact of the breach on the natural persons, and to promptly restore the availability of and access to the personal data.

10. Notification to the Data Subject

Should the risk level arising from the personal data breach as a result of the assessment discussed in paragraph 5.3 be high or very high for the rights and freedoms of the natural person whose data have been affected by the event, the data processor (where the conditions for not issuing the communication are not fulfilled) shall also report the event to the natural persons whose personal data have been affected by the breach. The notification seeks to enable the Data Subject to take the necessary precautions to mitigate potential negative effects and must be sent without undue delay.
The definition and drafting of an adequate communication to the Data Subjects affected by the breach shall consider the following:

- the information necessary and suitable for the context that shall be provided to the Data Subject;
- the execution procedures.

The communication to the Data Subjects shall contain, at least:

- a description of the nature of the personal data breach;
- a description of the probable consequences of the personal data breaches;
- a description of the measures implemented or suggested for implementation in order to remedy to the personal data breach and, if applicable, to reduce any negative effects;
- the name and contact details of the Data Protection Officer or another contact person that may provide further information;
- where possible or in the event of a specific suggestion from the Supervisory Authority, a list of good practices and/or specific measures to be implemented by the natural persons affected by the breach, in order to reduce the negative consequences;
- any other information deemed useful.

The listed contents shall be forwarded to the Data Subject by direct channels (e.g. e-mail, text message), providing a clear, transparent and detailed communication. The choice of the means of communication shall consider the Data Subject's ability to access different formats and, if necessary, the different languages spoken by the recipients.
Based on the specific circumstances of the case, the means of communication to be chosen shall be that capable of maximising the Data Subject's receipt of the information in a correct, simple and convenient manner, and, simultaneously, ensuring the security of the information transfer.
The communication shall be issued as soon as reasonably possible, taking into account the relevant guidelines laid down by the Supervisory Authority, the consequences that may arise from the specific context of the breach, as well as from the nature of the data and the purpose of processing, the consequences that may affect the management of the accident and containment of the breach.

The Company shall not be obliged to communicate the breach to the Data Subjects if one of the conditions below is satisfied:

- the appropriate technical and organisational protection measures have been implemented and such measures have been applied to the personal data subject to breach, especially the measures intended to render the personal data unintelligible to any person unauthorised to access them (e.g. encryption);
- the data processor, following the identification of the event, has promptly adopted measures intended to prevent the occurrence of a high risk for the rights and freedoms of the Data Subjects;
- should the means of direct communication require a disproportionate effort for the Data Processor whose data have been affected by the breach, the processor may adopt means of public communication provided that said means are efficient in terms of correctness and transparency and that they cause no further damage to the privacy of the Data Subject.

11. Data Breach Log

Pursuant to the Regulation, the data processor shall record in a Breach Log any personal data breach, including the circumstances related thereto, its consequences and the measures implemented to remedy it. Such documentation will allow the Authority to verify the compliance of the assessments, precautions and decisions taken with Article 33 of the GDPR.

Said document is kept and implemented by the Privacy Expert or, on his or her behalf, by the CIO, who shall guarantee the completeness, updating and integrity of the information enclosed therein.
It should be noted that, if the event reported is not assessed as personal data breach, the reasons for this assessment must be provided.

Attachment E – Data Retention Policy

1. Introduction & Purpose

This Data Retention Policy (the "Policy") sets out the legal requirements that all employees and agents (hereinafter, the "Recipients") must adhere to with reference to personal data retention periods to ensure the Group companies' compliance Group with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the "General Data Protection Regulation" or "GDPR").

2. To whom does this Data Retention Policy apply?

This Policy applies to:

a) all documents, archives or records created (hereinafter, the "Documents") or received by the Group, regardless of the means or format used (e.g. electronic, e-mail, images, hard copy, etc.) which contain personal data;
b) all physical locations where the Documents are stored (including structures operated by any service providers);
c) all employees and agents of any business unit of the Group and its suppliers.

Where a specific document, archive or record is not referenced in this Policy, the following general principles should be observed:

a) personal data should only be retained for as long as is necessary to satisfy the purposes for which it was collected;
b) where the personal data in a Document is deleted, or otherwise anonymised, the Document may be retained for a longer period of time (subject to restrictions imposed by legal provisions or any reductions due to the sensitivity of the document);
c) it is generally forbidden to retain Documents indefinitely, except in very specific circumstances.

d) Where can I get more information about this Policy?

For any clarification on this Policy, you can contact the Group's Privacy Expert at the following address privacyexpert@falckrenewables.com

e) Data Destruction

Documents that have been kept beyond the retention periods set out in the table below may be destroyed, if approved by the Privacy Expert. In any case, the premature destruction of Documents is expressly prohibited.

DATA RETENTION TABLE

Description of the legislative provisions regarding data retention	**Nature of documents containing personal data**	**Retention period**	**Notes**
GENERAL PRINCIPLE — Limits on the retention of personal data	Any document containing personal data.	Documents must be kept in such a form that allows identification of the data subjects for no longer than is necessary for the purposes for which the data were collected or processed. However, if the applicable regulations provide for a longer retention period, the latter shall take precedence.	This principle applies to any data processing. In cases of contracts containing personal data, it is advisable to keep the Documents for up to 10 years following the termination of the agreement in question as evidence in case of disputes.
HEALTH AND SAFETY			
Work equipment verification log.	The log regarding work equipment shall contain a description of the conservation status of the work equipment.	Indefinitely. The document must always be available in case of inspections by the authorities.	

Duty to keep a log of employees' exposure to hazardous substances and any accidents relating to employees that may carry out dangerous work or work in unhealthy environments (i.e. work that entails the use of dangerous substances).		Until the termination of the contractual relationship. However it is advisable to (i) ensure the logs are periodically updated (ideally once per year) and (ii) keep the logs for at least 10 years after the termination of the working relationship.	This log shall be provided to the competent authorities in the event of inspections.

Duty to draft a risk assessment for work equipment and chemical substances or mixtures used. The risk assessment seeks to identify: (i) the existence of any risk for the health and safety of employees during work activities; (ii) the prevention and protection measures implemented and the personal protective equipment adopted; (iii) the plan of the measures deemed suitable for ensuring the improvement of safety levels over time; (iv) the list of procedures that allow the implementation of the relevant measures; (v) the name of the Prevention and Protection Service Manager, the workers' safety representative or local representative and the company doctor who	Documentation regarding the risk assessment.	Indefinitely.	

participated in the risk assessment, (vi) the list of activities that could expose workers to specific risks that require recognised professional expertise.			
Duty to keep all data relating to employees' medical examinations, where necessary.	Register of employees' medical examinations.	There is no clear indication as to the retention times for this document. However, it is advisable to (i) have the registers periodically updated (ideally once per year), and (ii) keep them for at least 10 years after the termination of the employment relationship.	
ACCOUNTING and AUDITING/CORPORATE LAW			
Duty to keep accounting records and entries and business correspondence.	Accounting records, and business correspondence (e.g. the day book, auxiliary books, supporting documents that show the important elements of the accounting entries and all written material sent, received or internal which relates or is relevant to accounting).	10 years from the date on which those documents are drafted — save for longer periods as a consequences of (i) tax assessments and (ii) legal proceedings involving a request to submit such documents.	The applicable provisions of the Italian Civil Code on the methods of drafting the accounting books and entries shall be respected.
INTELLECTUAL PROPERTY RIGHTS			

Duty to keep documents regarding trademarks, patents, domain names, industrial secrets, etc.		There is no specific retention period for documents relating to intellectual property rights. However, for evidentiary purposes, it is advisable to keep the documents indefinitely (e.g. trademark registration certificates, patents)	
ANTI-MONEY LAUNDERING			
Duty to keep documents, data and information useful to prevent, identify or verify possible money laundering activities or the financing of terrorism and to allow the execution of the relevant analyses conducted, under their respective remits, by the Financial Intelligence Unit or other competent authorities.	Documents and data collected during the verification of customers and/or suppliers.	10 years from the termination of the relationship.	

HR DOCUMENTS			
Duty to keep (i) employees' data (i.e. name, surname, tax code), (ii) the total number	Employees' record books.	5 years from the last registration entry.	During the retention period, the data shall be retained in

of employees and the corresponding professional levels, (iii) their insurance positions.			compliance with the applicable data protection laws. Data/documents relating to former employees shall be included in an electronic folder accessible exclusively by the head of the human resources department or another party expressly appointed by him or her and by the Board of Directors and any other authorised corporate governance bodies.
Duty to keep all data relating to hiring procedures the employment relationship.	Hiring procedures, employment contracts and all associated documentation.	There is no specific provision in this respect. However, it is advisable to keep them for at least 10 years after the termination of the employment relationship. Candidates' data shall be stored, for applications submitted for specific positions, for up to 12 months from the completion of selection, and for up to 24 months from the date of collection of the data for spontaneous applications.	
Duty to keep all data relating to the social security contributions paid for employees.	Payslips and other records relating to payments.	Payslips and similar documents relating to employees' remuneration shall thus be kept for a period of 5 years from the date of the last entry. However, it is advisable to keep such information for at least 10 years after the termination of the employment relationship.	
Without prejudice to other different specific provisions,	Other employees' data.	To protect the interests of the company in case of claims by employees after termination of their employment	

the employees' personal data (including those contained in the employment contracts and said contracts themselves) must be retained for a period no longer than necessary for the purposes for which the data have been collected.		relationship, it is advisable to keep the data for at least 10 years after the date of termination of the employment relationship.	
Duty to keep all data relating to Social Security and Tax deductions made and/or contributions paid.	Documents relating to social security, insurance and tax deductions.	This information shall be kept for a period of 5 years. However, it is advisable to keep it for at least 10 years after the termination of the employment relationship.	
Duty to keep all data relating to (i) family status certificates and documents relating to family allowance, and (ii) any payments made to the I.N.A.I.L for insurance against workplace accidents.	Family status certificates and documents relating to the family allowance, and (ii) any payments made to the social security institutions	This information shall be kept for a period of 5 years. However, it is advisable to keep it for at least 10 years after the termination of the employment relationship.	
Limit on the conservation of CCTV images.	Footage of individuals.	24 hours following the recording of the footage, unless an additional retention period is required in specific situations, such as holidays or closing of the offices or businesses, or a specific investigation request has been made by the legal authorities or judicial police, which must be fulfilled.	
Limit on the retention of e-mail messages of former employees	Messages in the e-mail inbox of former employees.	For incoming/outgoing e-mails of a former employee: 3 months from termination of the employment relationship to ensure continuity of work and *company business.* Only for messages archived by the former employee within the document management system, to the extent significant for business	

		continuity: 10 years from termination of the employment relationship. In the event of proven, concrete requirements to protect or exercise a right of the Company in legal our out-of-court proceedings, or requests from the authorities for the purpose of concluding the last instance of proceedings and/or conclusion of the out-of-court phase and, in any event, no more than 10 years from termination of the employment relationship.	
Limit on the retention of the personal data of employees collected through access badges	Access data via badge Access data via badge.	5 years from collection. 5 years from collection.	
Duty to keep all data relating to employees' attendance at work.	Employees' attendance record book.	5 years from the last entry.	
DOCUMENTS RELATING TO MARKETING ACTIVITY			
Data collected for marketing purposes.	Any relevant document.	There is no specific provision in this respect. However, in accordance with the general legal approach, it is possible to retain such data, subject to the data subject's consent, for a period of 24 months following the collection thereof.	
Data processed for profiling purposes.	Any relevant document.	There is no specific provision in this respect. However, in accordance with the general legal approach, it is possible to retain such data, subject to the data subject's consent, for a period of 24 months following the collection thereof.	
SYSTEM LOGS			
Registration of system logs.	Electronic files.	The data retention period is 6 months from the time of collection.	