



## RED Privacy Policy

**Responsible Department** Legal, Ethics & Compliance and Data Privacy  
**Last Updated [Date]** 02 April 2024  
**Revision** Rev 1  
**File Ref** RED Privacy Policy  
**Classification**  Public |  Internal |  Restricted |  Confidential

# Revision

REVISION	REVISION DETAILS / ISSUE TYPE	PAGE NOS	DOCUMENT PREPARED BY			DOCUMENT CHECKED BY		
			NAME	SIGNATURE	DATE	NAME	SIGNATURE	DATE
REV 01	New Document	21	G Matthews		28.03.24	E Bentley		28.03.24

Red Engineering Design Limited accepts no responsibility or liability to any other party (exception for death and personal injury) in respect of or arising out of or in connection with this document and/or its contents.

**Copyright:**

The copyright of this document is vested in Red Engineering Design Limited. This document may not be reproduced in whole or in part without their express written permission.

# Contents

1.0	EXECUTIVE SUMMARY .....	1
2.0	DEFINITIONS.....	2
3.0	APPLICATION & GOVERNANCE .....	4
3.1	Application.....	4
3.2	Governance .....	4
4.0	TECHNICAL MEASURES .....	7
5.0	ORGANISATIONAL MEASURES.....	8
6.0	DATA PROCESSOR OBLIGATIONS.....	10
7.0	SPECIAL CATEGORY PERSONAL DATA .....	11
7.1	Criminal convictions and offences .....	11
7.2	Children .....	12
8.0	PRIVACY BY DEFAULT AND DESIGN .....	13
9.0	CONTRACTS .....	14
10.0	INTERNATIONAL TRANSFERS .....	15
11.0	ENGIE BINDING CORPORATE RULES .....	16
12.0	AWARENESS AND TRAINING .....	17
13.0	DATA SUBJECT RIGHTS .....	18
14.0	INCIDENTS AND BREACHES.....	19
	APPENDIX - RACI MATRIX.....	20

# 1.0 Executive Summary

RED is committed to protecting Personal Data and privacy, which are values set out in the ENGIE Group Ethics Charter. We process Personal Data relating to employees, clients' employees, contractors, partners, service provider and supplier employees in the course of our daily activities. We also process Personal Data to meet statutory requirements.

Our stakeholders (including our current and prospective employees, our clients, and the ENGIE group) expect us to meet high standards. Failure to do so through inadequate internal or external Processing or sharing of Personal Data, can lead to a loss of confidence by both employees and clients as well as the risk of significant regulatory fines and penalties.

Consequently, RED has mandated compliance with this Privacy Policy (the RED Privacy Policy) to underpin its activities and support the fair and lawful collection and usage of Personal Data by all the legal entities comprised within the RED Group. It is a key component of our accountability framework, requiring local RED entities in the countries where we are represented to implement this RED Privacy Policy and associated procedures based on the acknowledged high standards of the General Data Protection Regulation (GDPR) regardless of whether they fall within its purview legally. (A respecter of local differences, any local, national or regional regulation setting a higher bar in respect of any aspect of data protection is also to be met by the relevant RED Entity.)

This RED Privacy Policy does not sit in isolation but forms part of a much broader data governance and accountability regime. Personal Data must also be protected by following the [RED policies and procedures](#). These requirements are to be met prior to the effective implementation of and throughout the life cycle of any Processing of Personal Data. In particular, the planning of any project involving Processing or sharing of any Personal Data should incorporate the principles of Privacy by Default and Design (see section 7.0 below).

Compliance with the RED Privacy Policy ensures RED is legally compliant and meeting the expectations of our stakeholders.

This Policy was adopted by the Global Operations Board of RED on 15 March 2024.

## 2.0 Definitions

**Adopted** – Date the policy was first approved by the Global Operations Board of RED.

**Anonymisation** – Any information related to a natural person where the person cannot be identified whether by the Data Controller or by any other person, taking account of all the means likely reasonably to be used either by the Controller or by any other person to identify that individual (including reversibility of any anonymisation process).

**Binding Corporate Rules (BCRs)** – The set of internal rules ratified by the European Data Protection Board (in relation to the GDPR) or relevant Regulator (other legislation) which enable the free transfer of (some types of) Personal Data within the Group.

**Breach** – The accidental or unauthorised destruction, loss or alteration of Personal Data or its unauthorised disclosure or access.

**Data Controller** – The natural or legal person responsible for determining the purpose and methods of the Data Processing that have been implemented or are to be implemented. The Data Controller is bound to take every precaution necessary to ensure Data Privacy.

**Data Processor** – (Sub)contractor to whom the Data Controller assigns all or part of the operations relating to its Data Processing, such as implementation, hosting, operation, data management, etc.

**Data Protection Impact Assessment** – A systemic identification and assessment of the risks to the Data Subject of a system, application or process which helps the mitigation or erasure of that risk, and enables RED to demonstrate compliance with data protection obligations.

**Data Subject** – An identified or identifiable, living individual whose Personal Data is being processed by a Data Controller or a Data Processor.

**Encryption** – The process of encoding messages or information in such a way that only authorised parties can read it.

**Entity** – Legal entity within the consolidated scope of the Group.

**European Economic Area (EEA)** – The countries of the European Union and the member states of the European Free trade Association, plus the UK. (While the UK is not actually a member of the EEA, the close alignment of its data protection laws with those of the EU and ruling of equivalency make the application of this Policy easier if it is seen as an EEA member.)

**EU Processing Entity** – Entities established in the European Union or the UK, or processing the Personal Data of European Union or UK residents such that they fall within the scope of the GDPR or UK GDPR respectively by virtue of Articles 2 and 3.

**Personal Data** – Any information relating to an identified or identifiable living individual. This can include data subject to Pseudonymisation and opinions (unless excluded by local law). Anonymised data is not Personal Data.

**Personal Data** – Any information relating to an identified or identifiable living individual. This can include data subject to Pseudonymisation and opinions (unless excluded by local law). Anonymised data is not Personal Data.

**Processing** – Any operation or set of operations involving Personal Data, whatever the method or means used (automated Data Processing such as IT applications, Excel data files, etc., or non-automated Data Processing included or intended to be included in a structured filing system whereby Personal Data are

accessible according to specific criteria such as employees' individual paper files, etc.), particularly collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or other form of circulation, alignment or consolidation, blocking, deletion or destruction.

**Pseudonymisation** – is the separation of data from direct identifiers so that linkage to an identity is not possible without additional information that is held separately. Pseudonymisation, therefore, may significantly reduce the risks associated with Processing, while also maintaining the data's utility.

**RED/RED Group** – The group of companies within the control and common management of RED.

**RED Entity** – An Entity within the RED Group of companies.

**Regulator** – Body appointed by law to regulate or monitor compliance with data protection legislation, including supranational bodies such as the European Data Protection Board, and references to Regulators are to be read as relevant Regulators only.

**Rights** – The data protection rights given to Data Subjects by law such as the right of access; the right to object; the right of erasure; the right to rectification; the right to restrict processing, and the right to data portability. It can also include rights in relation to automated data processing.

## 3.0 Application & Governance

### 3.1 Application

This Policy is applicable to all employees and contractors of RED where we are the Data Controller. It sets out our approach in relation to privacy and the protection of personal data.

Non-compliance with this Policy may result in disciplinary action.

### 3.2 Governance

Data protection legislation operates on the basis of legal entity (company) whereas the ENGIE Group is organised on the basis of Global Business Units, Hubs, and Business Entities (GBU/Hub/BEs) with no recognised legal persona. This RED Privacy Policy provides a governance structure that bridges this by providing a common approach to privacy to be applied by all legal entities in the RED group.

References to local laws shall include as appropriate the laws of regional bodies such as the European Union, as well as national, federal, state or territory legislation or regulation. Capitalised terms specific to this policy are defined as met or in section 1 Definitions above.

#### 3.2.1 ENGIE and RED

This RED Privacy Policy follows the [ENGIE Group Data Privacy Policy](#) (the ENGIE Group Privacy Policy) which states that the strategic management of Personal Data protection and privacy has been delegated by the ENGIE Executive Committee to the Executive Vice President Group Corporate Secretary and the Executive Vice President IT and Digital. In turn, they have delegated responsibility for monitoring of the ENGIE Group Privacy Policy to the ENGIE Group Data Privacy Manager and coordinating its effective implementation through the Chief Legal Officer and the Data Privacy Manager of the GBU/Hub/BEs.

Within the RED Group, overall responsibility lies with RED's General Counsel. A summary of the main data protection responsibilities and accountabilities is given in the RACI Matrix in the Appendix below.

#### 3.2.2 Tractebel

As part of the Tractebel Business Entity, RED will follow all relevant guidance from Tractebel's Chief Legal, Ethics and Compliance Officer and/or Data Privacy Manager. Applicable Tractebel data protection policies and procedures are also to be followed with required reporting made.

Any deviation must first be reported to and agreed by RED's General Counsel who will discuss it with Tractebel's Chief Legal, Ethics and Compliance Officer and/or Data Privacy Manager.

#### 3.2.3 RED's General Counsel

The main duties of RED's General Counsel in relation to data protection and privacy are to:

- Ensure the effective implementation of the [ENGIE Group Privacy Policy](#) and the RED Privacy Policy, including monitoring their application.
- Ensure that regulations governing Personal Data are respected within RED.
- Establish a privacy programme and reporting on it (including to Tractebel or the ENGIE Group as required).
- Support accountability requirements by establishing a framework to support:
  - Data protection governance (including setting up relevant procedures)
  - Employee training and compliance support
  - Compliance with legal obligations including Rights

- Handling of Personal Data Breaches/Rights
- Awareness of the ENGIE Group's BCRs.
- Coordinate data protection related activities across RED including in relation to Data Protection Impact Assessments on relevant cross-group projects, systems, applications, and processes.
- Represent RED to Tractebel or the ENGIE Group on privacy matters, including coordinating any required ENGIE Group reporting and liaising with the Tractebel Chief Legal, Ethics and Compliance Officer/Data Privacy Manager.
- Providing advice on data protection matters and good practice to RED.

### 3.2.4 Local Data Privacy Champions

With the exception of the UK which shall be covered by RED's General Counsel, each country in which RED has an entity or an establishment, shall nominate a Local Data Privacy Champion. If, after discussion with the RED Entity senior management, a suitable individual is not nominated (or fails to fulfil the role), RED's General Counsel will nominate an individual.

The role of the Local Data Privacy Champion is to provide an internal focal point for discussions and actions in relation to data protection and privacy. The Local Data Privacy Champion is not expected to be an expert in data protection and privacy but is responsible for ensuring that their RED Entity is aware of its data protection responsibilities and supporting compliance by:

- Ensuring awareness of data protection requirements and expected behaviours in the RED Entity including those in the RED Privacy Policy.
- Supporting data protection compliance activities, including awareness campaigns and other activities organised by RED's General Counsel, Tractebel Data Privacy Manager or ENGIE Group Data Privacy Manager.
- Ensuring that RED's General Counsel is made aware of all potentially relevant matters (including non-compliance with requirements) and making sure that all relevant questions are referred.
- Acting as the central liaison point in the RED Entity for data protection matters.
- Acting as the liaison point for relevant Regulators (including registering with them) where specifically requested by RED's General Counsel.
- Actively participating in the Tractebel Data Privacy Network and relevant training sessions.
- Producing reports on data protection matters in the RED Entity and contributing to those of the RED Group/Tractebel as appropriate.

A Data Privacy Manager may be appointed to support multiple entities, countries or larger RED Entities. The role of the Data Privacy Manager is similar to that of the Local Data Privacy Champion but the Data Privacy Manager is expected to dedicate more of their time to data protection; be more knowledgeable, and more proactive.

References to the Local Data Privacy Champions in this RED Privacy Policy shall include Data Privacy Managers where appointed.

### 3.2.5 RED's Global Operations Board

The Global Operations Board is ultimately responsible for the day-to-day management of the business including for compliance with data protection regulation and this RED Privacy Policy. It shall receive regular reports on Data Protection activity and advise on issues. It is responsible for ensuring that RED's General Counsel is given the necessary resources and time to fulfil the mission assigned.

### 3.2.6 Information Security

RED's Head of Information Security and the cyber security team shall work with RED's General Counsel and the Local Data Privacy Champions in ensuring that:



- appropriate technical measures as required by law are in place by offering their expertise and support in the area of data privacy, both for the purposes of data processes hosted internally and those hosted by a third party; and
- the reporting and remediation of any data security breaches relating to IT systems and equipment.

### 3.2.7 RED Senior Leadership

All managers in RED are responsible for:

- Understanding their data protection responsibilities.
- Ensuring that data protection requirements are observed throughout their work area and by their staff (including being familiar with the contents of this RED Privacy Policy).
- Providing clear messages to their employees regarding appropriate processing of the personal data that they handle, ensuring that:
  - any Personal Data which they deal with is kept securely;
  - Personal Data is not disclosed orally or in writing or otherwise to any unauthorised third party;
  - they and their staff do not send Personal Data outside of RED (including to clients) without express authority unless it is a normal part of their role;
  - adequate written processes and procedures are in place and followed by their teams to ensure fair processing of Personal Data;
  - training needs within their team are identified and raised with the Local Data Privacy Champion (or Information Security if relating to data security).
- Adopting measures to ensure the integrity of staff through selection, training, supervision and motivation. This includes non-permanent staff permitted access to Personal Data.
- Consulting with the Local Data Privacy Champion before Processing Personal Data for a new or significantly different purpose to that for which it was originally collected.
- Promptly sending any exercise of Rights, complaints or enquires relating to the treatment of Personal Data to the Local Data Privacy Champion, and informing the Local Data Privacy Champion of any Breaches or potential Breaches as soon as the manager becomes aware.

Any manager who is faced with a request or situation involving the disclosure of Personal Data not covered by this RED Privacy Policy, the Processing of Personal Data which is not in accordance with normal practices, or anything else which causes concern or requires further guidance must immediately contact their Local Data Privacy Champion or RED's General Counsel.

### 3.2.8 RED Employees

All staff (whether temporary or permanent) are responsible for:

- Understanding their data protection responsibilities in relation to their job.
- Understanding and complying with this RED Privacy Policy, associated guidance, processes and procedures as well as other relevant policies.
- Contacting their Local Data Privacy Champion for guidance if they are in any doubt about how they should deal with any Personal Data.
- Only processing Personal Data in the manner that is authorised for the purpose of carrying out their job or with management authorisation.
- Ensuring any Personal Data with which they deal is kept securely and in accordance with all relevant policies, procedures, processes, and guidance.

Not disclosing orally or in writing or otherwise to any third party any Personal Data unless authorised to do so. RED Personal Data must never be communicated by personal email or non-IT approved channel.

## 4.0 Technical Measures

All appropriate protective measures must be taken with regards to the nature of the data, generally accepted practice, and the possible negative consequences to the Data Subject presented by the Processing to ensure that Personal Data is secure and kept confidential, in particular, to protect them from being distorted, damaged or lost, and prohibit unauthorised access. To ensure the security and confidentiality of processed Personal Data, measures such as Pseudonymisation, Anonymisation and Encryption should be considered. Measures adopted should cover data in transit as well as at rest. Test environments using live Personal Data (as opposed to dummy or anonymised data) must also comply with this RED Privacy Policy and relevant Data Protection laws.

The appropriateness of technical measures should be regularly reviewed with due regard given to advances in technology and changes in legislation or law.

All appropriate mitigations should be taken when Processing Personal Data to ensure it is kept secure and confidential, in particular to protect it from being distorted, damaged, lost and to prohibit unauthorised access.

To ensure the security, all access controls are to be reviewed no less than annually to ensure that they are operating correctly and that only those people who should have access do.

## 5.0 Organisational Measures

Organisational measures must be put in place to ensure that all Personal Data is processed in accordance with relevant Data Protection laws and stakeholder reasonable expectations. These measures can consist of controls (such as segregation of duties, supervisory checking and access controls), written processes and procedures or guidance, training and reviews or audits.

The organisational measures put in place shall ensure the effective implementation of the following principles:

**(a) *Processing shall be proportionate in relation to the legitimate purpose pursued and always reflect a fair balance between all concerned interests and the rights and freedoms at stake***

Before any new Processing is undertaken, the proportionality must be considered, including whether the Processing is actually needed, and, except where there is a statutory obligation, whether the benefits to RED outweigh the risks to the Data Subjects.

**(b) *Personal Data shall be processed lawfully, fairly and transparently***

Personal Data must be collected and processed by fair means for specified, explicit and lawful purposes and must not be used or processed subsequently in a way that is incompatible with these purposes.

The Data Subject must be informed of the Processing in a Privacy Notice which sets out in a clear and transparent way what Personal Data the RED Entity has collected; how it will be used, and how a Data Subject can contact the RED Entity to exercise their legal rights together with other information required by law.

**(c) *The Processing must be carried out on the basis of a legitimate interest laid down by law and the personal data collected shall not be further processed incompatibly with those purposes***

RED must identify and record the reason why it obtains and processes the Personal Data. The following are generally legally permitted purposes (lawful bases of Processing):

- The Data Subject has agreed to Processing for a specific purpose (consent).
- It is necessary to give effect to a contract with or implement a request from the Data Subject.
- It is required by law.
- It protects the Data Subject or another individual's vital interests.
- It is necessary for RED's legitimate interests, and does not impact the fundamental rights and freedoms of the individual.
- It is necessary for medical reasons (including pre/during employment assessments).<sup>1</sup>
- The data has already been made public.

Where the basis is consent, the consent must be a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the Data Subject's agreement to the Processing of their Personal Data such as by a written statement (including by electronic means) or an oral statement and must be clear, explicit, and unequivocal. Proof of consent must be retained in case of challenge by a Data Subject or query by a Regulator. Such consent can be withdrawn at any time by the Data Subject (who must be advised of this fact at the same time as giving the consent).

---

<sup>1</sup> This does not apply to a child unless explicitly legally permitted.

Any new processing for a different purpose cannot occur until the lawful purpose is identified (and, if based on consent, the Data Subject has agreed to it).

**(d) *Personal Data must be adequate, relevant and not excessive in relation to the purposes for which it is processed***

Under the principle of minimisation, the Personal Data collected must be adequate, relevant and limited to what is strictly necessary for the purposes for which the Personal Data is processed.

Staff developing application forms, questionnaires, and any other forms for collecting Personal Data must ensure that no more information is sought than is necessary. Essential and optional data fields must be clearly marked as such. Procedures and forms should be regularly reviewed to ensure that Personal Data does not continue to be collected unnecessarily.

Personal Data must not be collected or retained on the basis that it may prove useful for an undefined purpose in the future. Anonymise or abbreviate Personal Data if it is possible to do so in relation to the purpose for which it is held, for example when analysing responses to a questionnaire.

**(e) *Personal data shall be accurate and, where necessary, kept up-to-date***

Efforts should be made to ensure that both the initial Personal Data captured and the Personal Data held is accurate and regularly reviewed particularly if decisions concerning the Data Subject are made based on it.

**(f) *Personal data shall not be preserved in a form which permits identification of data subjects for any longer than is necessary for the purpose(s) for which the data is being processed***

All applications, systems and processes which hold Personal Data shall have a definitive retention end date covering the Personal Data held within them. The retention period of the processed Personal Data must be defined in accordance with the purpose of the collection and with regard to applicable laws. Personal Data is to be permanently deleted, anonymised, or disposed of securely at such end date. This includes archived data and paper copies. It is therefore advisable to organise the automatic or manual deletion of data based on pre-defined retention periods.

**(g) *Personal data undergoing processing is subject to appropriate safeguards. When processing Special Category Personal Data, such safeguards shall guard against the risks that such processing may present to the rights and fundamental freedoms of the data subject, including the risk of discrimination***

All applications, systems and processes shall respect the rights of the Data Subjects (section 13.0). Additionally, any automated decision making (where this is not reviewed by an employee for a final decision) shall be advised to the Data Subject.

All staff have a duty to protect Personal Data. Managers must ensure that staff are aware of and comply with security procedures. This includes non-permanent staff permitted access to Personal Data.

Clearly written procedures shall be implemented. Access controls, both physical and system based, must be implemented and appropriate audit trails put in place in all areas where there is Personal Data Processing. Paper copies should not be held unless strictly necessary.

Cyber Security Policies and Procedures must be followed at all times.

## 6.0 Data Processor Obligations

Any RED Entity which subcontracts Data Processing to a Data Processor remains legally responsible for the protection of the Personal Data (in the majority of jurisdictions). RED Entities must ensure that these contractors/suppliers process the data in accordance with the protection principles of this RED Privacy Policy.

Data Processors must be selected for their ability to respect Data Protection legislation as well as any commercial factors. A written contract must be concluded providing for the Data Processor's obligations to comply with Personal Data protection rules including confidentiality and security measures. Appropriate due diligence must also be done on any prospective Data Processor to ensure its suitability.

## 7.0 Special Category Personal Data

Some types of Personal Data are deemed to be Special Category and require additional care and controls. These are generally intimate details or are likely to give rise, in case of misuse, to unlawful or arbitrary discrimination.

The following types of Personal Data are to be deemed Special Category Personal Data. Information concerning:

- Racial or ethnic origins
- Generic or biometric data
- Political opinion or affiliation
- Mental or physical health
- Trades union membership
- Sexual orientation or activity
- Religious or philosophical beliefs (including lack of belief).

Applicable local or regional laws may add other types of Personal Data to the above list e.g. social security or identity card numbers. Relevant laws can include labour fiscal laws as well as data protection legislation. If in doubt, these types of Personal Data are to be treated as Special Category Personal Data to ensure lawful Processing. Staff likely to Process such Personal Data must make themselves aware of relevant restrictions or prohibitions to prevent any breach or unlawful Processing.

Additional levels of control and technical/organisational measures are required for the processing of Special Category Data. Where permitted, access should be kept to the minimum level of staff necessary.

Special Category Personal Data may only be processed by RED as Data Controller where:

- RED has recorded explicit consent of the Data Subject (where permitted to override any legal prohibition).
- The processing is mandated by or otherwise permitted by law.
- It is necessary to protect the vital interests of the Data Subject or another individual (i.e. in an emergency; public health; cross boarder travel).
- It is necessary to carry out preventive or occupational health, including assessments.
- The Special Category Personal Data has been made public by the Data Subject (e.g. social media site postings with public settings).
- It relates to litigation.
- It relates to archiving supporting statistical analysis (where permitted).

The above requirements are additional to the lawful basis of Processing listed in section 5.0(c) above i.e. both need to be satisfied even if only Special Category Personal Data is being processed.

Particular care is required in relation to the following types of Processing:

- Processing likely to exclude an individual from enjoying a right, benefit or contract;
- Processing involving the interconnection of files having different purposes;
- Processing involving the international transfer of Special Category Personal Data outside the ENGIE Group.

### 7.1 Criminal convictions and offences

Where Processing is permitted, special care needs to be taken to comply with any relevant legal requirements restrictions (including those not directly related to data protection). Where there are no

specific restrictions or legal requirements, data on criminal convictions and police reports of good standing should be treated as Special Category Personal Data. Best practice requires a dedicated written procedure on handling this type of Personal Data. In all cases RED's General Counsel and local legal counsel must be consulted first.

## 7.2 Children

While the Personal Data of children is often not classified as Special Category Personal Data, it is to be given a similar treatment in terms of control, technical and organisational measures. Special care should be taken to respect any local legal distinctions/regulatory guidance about different age brackets.

## 8.0 Privacy by Default and Design

Privacy by design and default is a key part of both Data Protection laws and RED's stakeholders' expectations.

**Privacy by Design** – This concept ensures that the privacy rights of the Data Subject are considered at all stages of any data processing by reviewing the process and building specific technical and organisational measures to limit the impact on the Data Subject when a new process is being designed or an existing one amended/reviewed.

**Privacy by Default** – This is the operation of the appropriate technical and organisational measures as described in sections 4.0 and 5.0 above to ensure that only the Personal Data which is strictly necessary for the identified purpose(s) is processed.

RED Entities shall put in place and publicise appropriate procedures to ensure that their local systems, applications and processes meet the above, including undertaking any relevant risk assessments, such as Data Protection Impact Assessments.



## 9.0 Contracts

All agreements (whether internal or external) involving Processing must be in writing.

For EU Processing Entities and other RED Entities signing contracts which may cover EEA residents, such data processing agreements must also meet the requirements of Article 28 of the GDPR; section 10.0 below on International Transfers, and any relevant local Data Protection laws. All other contracts involving Processing should try to meet the above requirements. Where the agreement is RED as a Data Controller to a third party or Data Controller for the sharing of data as opposed to RED as the Data Controller to a Data Processor, RED's General Counsel shall support the RED Entities in understanding what Personal Data may be lawfully shared with others and any relevant restrictions on Processing. Any violation of these requirements is to be logged as a Breach.

## 10.0 International Transfers

Care should be taken with all potential transfers of Personal Data across national borders to ensure compliance with applicable legal requirements. The RED employee requesting the contract permitting the transfer is responsible for compliance by ensuring that the correct individuals are consulted, and any required steps undertaken.

The Local Data Privacy Champion must be consulted in advance for all potential transfers of Personal Data from the EU/UK to a country or territory outside of the EEA or where the RED Entity will be signing a contract with an entity which will or may transfer Personal Data outside of the EEA.

## 11.0 ENGIE Binding Corporate Rules

RED benefits from ENGIE's Binding Corporate Rules (BCR) which enable the free transfer of HR and IT related Personal Data across national borders within the ENGIE Group. All transfers of Personal Data covered by such BCR shall be made in accordance with the terms of the BCR. Any failure to comply is to be reported to the Local Data Privacy Champion as a Breach.

## 12.0 Awareness and Training

All RED employees are required to complete the mandatory Personal Data protection training (including refresher training at least every three years). Those employees whose job requires frequent processing shall receive further training and a record of said training kept.

The Local Data Privacy Champion shall raise awareness of personal data protection in their country and promote RED's initiatives and trainings.

## 13.0 Data Subject Rights

Data Subjects have contingent rights to ensure that RED is respecting the data protection principles outlined in section 5.0 above, namely the right of processing confirmation/access; the right to object; the right of rectification; the right of erasure, and the right not to be adversely impacted by fully automated decision processes with no ability to appeal to a human.

RED Entities therefore need to ensure that all employees are aware of and can recognise these rights and follow the appropriate RED's procedures to ensure that legal rights and timeframes are respected. The Local Data Privacy Champion and RED's General Counsel are to be advised immediately on receipt of any expression of the exercise of these rights (written or verbal).

## 14.0 Incidents and Breaches

Any person being aware of a potential inappropriate use of Personal Data or Breach involving Personal Data shall immediately notify their Local Data Privacy Champion or RED's General Counsel directly. If alerted, the Local Data Privacy Champion will immediately inform RED's General Counsel.

For example, sending an email containing an individual's outstanding holiday entitlement to the wrong person; Personal Data details are lost or stolen; a file containing Personal Data is deleted by mistake; a system is hacked and Personal Data accessed; or a system failing and the Personal Data not being available.

RED's General Counsel will classify such event:

- **Minor Incident** – a Breach occurs but the quality of the Personal Data is low e.g. the name/job title of business contacts or an email containing Personal Data is sent to the wrong person, but the attachment was encrypted so that the recipient could not open it.
- **Moderate Breach** – a more significant Breach (e.g. a file containing Special Category Personal Data is sent to the wrong RED employee).
- **Major Breach** – a Breach involving a large volume of Personal Data or where there is a high risk to the fundamental rights and freedoms of the Data Subject(s) (e.g. a HR system is hacked; the salary details of a group of employees is erroneously sent to a third party).

The above classifications are to be assessed on the volume and quality of the Personal Data only. Commercial considerations may warrant further action which is outside of the scope of this RED Privacy Policy.

RED's General Counsel is responsible for any onwards notification at ENGIE Group level, and for informing Information Security.

Any formal Breach notification to a Regulator will be decided by RED's General Counsel after consultation with Tractebel's Chief Legal, Ethics and Compliance Officer, or where notification time restrictions permit, the ENGIE Group Data Privacy Manager. (This does not apply to local requirements to provide information on Breaches to a Regulator periodically.)

All Breaches are to be recorded in a central register held on RED's Legal Restricted Sharepoint with the following information recorded:

- date on which the event occurred (and date on which RED first became aware of the event if different);
- type(s) of Personal Data involved (including whether any Special Category Personal Data is involved and number of Data Subjects effected);
- summary of what occurred;
- root cause; and
- any mitigating factors/actions and anything else which is felt to be relevant.

Any decision to make a Breach public or to inform the affected Data Subjects clients will only be taken by RED's General Counsel after consultation with Tractebel's Chief Legal, Ethics and Compliance Officer (who shall consult within the ENGIE Group as appropriate).

All remediations are to be actioned within a timeframe agreed by RED's General Counsel, and progress is to be reported monthly to the RED Global Operations Board.

## Appendix - RACI Matrix

#	Activity	ENGIE Group DPM	Tractebel's Chief Legal, Ethics and Compliance Officer	RED's General Counsel
<b>1</b>	<b>Structure Data Privacy Compliance</b>			
1.1	Define ENGIE Group DP Policy	A/R	I	I
1.2	Define RED DP Policy	I	C	I
1.3	Organise RED DP Community	I	C	R
<b>2</b>	<b>Organise Privacy Compliance</b>			
2.1	Define and implement DP compliance programme	I	C	R
2.2	Implement necessary corrective DP actions		I	A/R
<b>3</b>	<b>Monitor Privacy Compliance</b>			
3.1	Monitor and report compliance in RED	I	C	R
3.2	Monitor and report local compliance		I	A/R
<b>4</b>	<b>Handle Data Breaches</b>			
4.1	Identify PD breach			A/R
4.2	Handle, alert and escalate	I	C	
4.3	Notify DPA when required	I	C	I*
4.4	Report breaches and lessons learned	I	I	R
<b>R = Responsible A= Accountable S = Supports C=Consulted I=Informed</b>				
* above corresponds to most circumstances but the local entity may be asked by the RED Chief Legal Officer to report the breach themselves if they have a local representative registered with the DPA				