DATA PROTECTION POLICY (THE "POLICY")

STRYTEN ENERGY LLC ("STRYTEN" OR "THE COMPANY")

You are required to read this policy because it provides important information about:

- the data protection principles with which Stryten must comply;
- what constitutes personal information (or data) and sensitive personal information (or data);
- how Stryten collects, uses and (ultimately) deletes personal information and sensitive personal information in accordance with the Policy;
- where more detailed information regarding the data can be found, e.g., the personal information Stryten gathers and uses, how the personal information is used, stored and transferred, for what purposes, the steps taken to keep that personal information secure and for how long it is kept;
- your obligations as a Stryten employee in relation to data protection; and
- the consequences of failure to comply with this Policy.

1 Introduction

1.1 Stryten obtains, keeps and uses personal information (also referred to as "personal data") about third parties for a number of specific lawful purposes, as set out in Stryten's data protection privacy notices.

1.2 This Policy sets out how we comply with our data protection obligations. The purpose of the Policy is also to ensure that staff, including employees, as well as temporary and agency workers understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.3 Stryten is committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information, and how (and when) we delete that information once it is no longer required.

1.4 If you have any questions or comments about the content of this Policy or if you need further information, you should contact the local GDPR Correspondent or the Legal Department.

2 Scope

2.1 Employees should refer to Stryten's data protection privacy notices and, where appropriate, to its other relevant policies including in relation to the information security and record retention, which contain further information regarding the protection of personal information in those contexts.

2.2 Stryten will review and update this Policy in accordance with our data protection obligations. This Policy does not form part of any employee's contract of employment and we may amend, update or supplement the Policy from time to time. We will circulate any new or modified policy to staff when it is adopted.

3 Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to a data subject who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or more generally using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify a data subject without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable data subject;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about a data subject's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify a data subject) and information concerning a data subject's health, sex life or sexual orientation.

4 Data protection principles

4.1 Stryten will comply with the following data protection principles when processing personal information:

4.1.1 we will process personal information lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;

4.1.5 we will keep personal information in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the information is processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5 Basis for processing personal information

5.1 In relation to any processing activity Stryten will, before the processing starts for the first time, and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, ie:

(a) that the data subject has consented to the processing;

(b) that the 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;

(c) that the processing is necessary for compliance with a legal obligation to which the Company is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person; or

(e) that the processing is necessary for Stryten's legitimate interests or those of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 5.2 below.

5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);

5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

5.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 6.2.2 below), and document it (for UK only); and

5.1.6 where criminal offence information is processed in accordance to Union or Member State law, also identify a lawful condition for processing that information, and document it.

5.2 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

5.2.1 conduct an appropriate legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

5.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);and
5.2.3 include information about our legitimate interests in our relevant privacy notice(s).

6 Sensitive personal information

6.1 Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.
6.2 The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if:
6.2.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above, e.g., it is necessary for the performance of an employment contract, to comply with Stryten's legal obligations or for the Company's legitimate interests; and
6.2.2 one of the special conditions for processing sensitive personal information applies, e.g.,:
(a) the data subject has given explicit consent;
(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of Stryten or the data subject;
(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;
(d) processing relates to personal data which are manifestly made public by the data subject;
(e) the processing is necessary for the establishment, exercise or defence of legal claims; or
(f) the processing is necessary for reasons of substantial public interest.

6.3 Sensitive personal information will not be processed by Stryten until:
6.3.1 the data subject has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.
6.4 The Company will not carry out automated decision-making (including profiling) based on any data subject's sensitive personal information.
6.5 The Company's data protection privacy notice sets out the types of sensitive personal information that Stryten processes, what it is used for and the lawful basis for the processing.
6.6 In relation to sensitive personal information, the Company will comply with the procedures set out in paragraphs 6.7 and 6.8 below to make sure that it complies with the data protection principles set out in paragraph 4 above.
6.7 During the recruitment process: Stryten's Human Resources Department will ensure that (except where the law permits otherwise):
6.7.1 during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, e.g., race or ethnic origin, trade union membership or health;
6.7.2 any completed equal opportunities monitoring form is kept separate from the data subject's application form, and is not be seen by the person shortlisting, interviewing or making the recruitment decision;
6.7.3 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

6.8 During employment: the Human Resources Department will process:
6.8.1 health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness

benefits;
6.8.2 sensitive personal information for the purposes of equal opportunities monitoring. Where possible, this information will be anonymised; and
6.8.3 trade union membership information for the purposes of staff administration and administering 'check off'.

7 Criminal records information

Criminal records information will be processed in accordance with the Union or Member State law.

8 Data protection impact assessments (DPIAs)

8.1 Where processing is likely to result in a high risk to a data subject's data protection rights (e.g., where Stryten is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:
8.1.1 whether the processing is necessary and proportionate in relation to its purpose;
8.1.2 the risks to data subjects; and
8.1.3 what measures can be put in place to address those risks and protect personal information.
8.2 Before any new form of technology is introduced, the manager responsible should therefore contact the Information Technology Department in order that a DPIA can be carried out.
8.3 During the course of any DPIA, the Company will seek the advice and the views of any other relevant stakeholders.

9 Documentation and records

9.1 Stryten will keep written records of processing activities, including:
9.1.1 the name and details of the Stryten legal entity (and where applicable, of other controllers);
9.1.2 the purposes of the processing;
9.1.3 a description of the categories of data subjects and categories of personal data;
9.1.4 categories of recipients of personal data;
9.1.5 where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;
9.1.6 where possible, retention schedules; and
9.1.7 where possible, a description of technical and organisational security measures.
9.2 As part of our record of processing activities we document, or link to documentation, on:
9.2.1 information required for privacy notices;
9.2.2 records of consent;
9.2.3 controller-processor contracts;
9.2.4 the location of personal information;
9.2.5 DPIAs; and
9.2.6 records of data breaches.
9.3 If we process sensitive personal information or criminal records information, we will keep written records of:
9.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
9.3.2 the lawful basis for our processing; and
9.3.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.
9.4 We will conduct regular reviews of the personal information we process and update our

documentation accordingly.

10 Data subjects' rights

10.1 Data subjects have the following rights in relation to their personal information:
10.1.1 to be informed about how, why and on what basis that information is processed—see Stryten's [data protection privacy notice];
10.1.2 to obtain confirmation that their information is being processed and to obtain access to it and certain other information, by making a subject access request;
10.1.3 to have data corrected if it is inaccurate or incomplete;
10.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');
10.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful; and
10.1.6 to restrict the processing of personal information temporarily where they do not think it is accurate, or where they have objected to the processing;
10.1.7 where legally required to set guidelines for the retention, erasure and communication of their personal data after death.

11 Data subjects' obligations

11.1 Individuals are responsible for helping Stryten keep their personal information up to date. You may have access to the personal information of other employees, suppliers and customers in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those data subjects. If you have access to personal information, you must:
11.1.1 only access the personal information that you have authority to access, and only for authorised purposes;
11.1.2 only allow other Stryten personnel to access personal information if they have appropriate authorisation;
11.1.3 only allow individuals who are not Company personnel to access personal information if you have specific authority to do so from the Human Resources or Legal Departments;
11.1.4 keep personal information secure (e.g., by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Company's Global Information Security Policy);
11.1.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
11.1.6 not store personal information on local drives or on personal devices that are used for work purposes.
11.2 You should contact the Human Resources Department or the Legal Department if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):
11.2.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information;
11.2.2 any data breach as set out in paragraph 15.1 below;

11.2.3 access to personal information without the proper authorisation;
11.2.4 personal information not kept or deleted securely;
11.2.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the Company's premises without appropriate security measures being in place;
11.2.6 any other breach of this policy or of any of the data protection principles set out in paragraph 4.1 above.

12 Data subject access

12.1 A data subject may make a request ("SAR") at any time to find out more about the personal data which the Company holds about them. The Company is normally required to respond to SARs within one month of receipt (this can be extended by up to two months in the case of complex and/or numerous requests, and in such cases the data subject shall be informed of the need for the extension).
12.2 All subject access requests received must be forwarded to the local GDPR Correspondent.
12.3 The Company does not charge a fee for the handling of normal SARs. Stryten reserves the right to charge reasonable fees for additional copies of information that have already been supplied to a data subject, or for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

13 Information security

13.1 The Company will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:
13.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;
13.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
13.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
13.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
13.2 Where the Company uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:
13.2.1 the organisation may act only on Stryten's written instructions;
13.2.2 those processing the data are subject to a duty of confidence;
13.2.3 appropriate measures are taken to ensure the security of processing;
13.2.4 sub-contractors are only engaged with Stryten's prior consent and under a written contract;
13.2.5 the organisation will assist Stryten in providing subject access and allowing data subjects to exercise their rights in relation to data protection;
13.2.6 the organisation will assist Stryten in meeting its obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
13.2.7 the organisation will delete or return all personal information to Stryten as requested at the end of the contract;
13.2.8 the organisation will submit to audits and inspections, provide Stryten with whatever

information the Company needs to ensure that both Stryten and the organisation are meeting their data protection obligations; and

13.2.9 the organisation will notify Stryten immediately if it is asked to do something infringing data protection law.

13.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by Stryten's Legal Department.

14 Storage and retention of personal information

14.1 Personal information (and sensitive personal information) will be kept securely in accordance with the Company's Global Information Security Policy.

14.2 Personal information (and sensitive personal information) should not be retained longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Employees should follow the Company's Records Retention Policy which sets out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the local GDPR Correspondent or the Legal Department.

15 Data breaches

15.1 A data breach may take many different forms, for example:

15.1.1 loss or theft of data or equipment on which personal information is stored;

15.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

15.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

15.1.4 human error, such as accidental deletion or alteration of data;

15.1.5 unforeseen circumstances, such as a fire or flood;

15.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

15.1.7 where information is obtained by deceiving the organisation which holds it.

15.2 The Company will:

15.2.1 make the required report of a data breach to the appropriate Supervisory Authority or Information Commissioner's Office (UK) without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of data subjects; and

15.2.2 notify the affected data subjects if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

16 International transfers

16.1 The Company may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to the Company's ultimate parent company, Stryten Energy LLC in the United States of America on the basis that Stryten Energy LLC is designated as having standard data protection clauses.

17 Training

The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are

responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

18 Consequences of failing to comply

18.1 The Company takes compliance with this policy very seriously. Failure to comply with the policy:

18.1.1 puts at risk the data subjects whose personal information is being processed; and

18.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Company; and

18.1.3 may, in some circumstances, amount to a criminal offence by the individual.

18.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

18.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact the GDPR Country Representative or the Legal Department.