ENERGUS.

DATA PROTECTION POLICY
(ENG-IMP01)

Version Control

	Version 2			
Date:	February 2018			
Prepared by:	Samantha Scott HR Officer			
Approved by:	Adrienne Easterbrook General Manager			

Data Protection Policy

ENERGUS.

ENG-IMP01

Contents

1. Scope

1.1 The General Data Protection Regulations (GDPR) provides individuals with rights in relation to personal data held/processed by organisations. The GDPR also place obligations on organisations to have appropriate technical and organisational measures in place to ensure the integrity and confidentiality of personal information held/processed.

1.2 Energus holds and possesses information about its staff, consultants, contractors and other stakeholders for various purposes including its obligations as a responsible and effective employer, in order to operate payroll and pension services. To comply with GDPR legislation, information must be collected and used fairly, stored safely, updated regularly and not disclosed to any unauthorised person or organisation.

1.3 Energus has a statutory obligation as a Data Controller/Processor to be responsible for and be able to demonstrate compliance with the legislation. All staff can obtain full details of Energus' processing from the Data Protection Officer (HR Officer).

1.4 This policy defines the responsibilities of Energus and its employees, contractors and consultants and ensures that all ae aware, not only of the requirements of data protection legislation on Energus itself, but also their individual responsibilities in this respect. A failure to comply with the provisions of GDPR may render Energus, or in certain circumstances the individuals involved, including the Energus Data Protection Officer (HR Officer) and the relevant responsible Manager(s), liable to criminal prosecution as well as giving rise to civil liabilities.

1.5 This policy must be read in conjunction with its corresponding procedure, ENG-IMP04 Subject Access Request Procedure (Data Protection), which details how Energus respond to requests for access to personal information.

2. Responsibilities and Definitions

2.1 The HR Officer is also the **Energus Data Protection Officer** and is responsible for ensuring that statutory and regulatory obligations with respect to the GDPR are adhered to and for the provision of training, guidance and advice to ensure policy compliance by all Energus employees, consultants and contractors. They are also the individual to whom all subject access requests and queries concerning personal data should be addressed.

2.2 **The Information Commissioner's Officer** is the UK's independent authority set up to promote access to official information and to protect personal information.

2.3 **Data Controller** is the person or organisation who determines the purposes for which personal data is to be processed.

2.4 **Data Processor** is any individual or company who records and/or processes personal date in any form on or behalf of Energus.

2.5 **Energus General Manager and Energus Managers** are responsible for the promulgation of this policy and any associated guidance within their own business unit.

2.6 **Energus permanent and temporary employees, contractors and consultants** are responsible for incorporating this policy and its associated documents into their own working practices.

2.7 **Data Processing** in relation to this policy means obtaining, recording, holding or carrying out any operation, or set of operations, on the information including;

- Collection, recording, organisation, structuring, storage;
- Carrying out any operation, or set of operations, on the information include:
  - organisation, adaptation or alteration of the information;
  - retrieval, consultation or use of the information;
  - disclosure of the information by transmission, dissemination or otherwise making available;
  - alignment, combination, blocking, erasure or destruction of the information.

2.8 **Data Subject** means any individual who is subject of personal data, an employee, contractor, consultant, stakeholder or third party about whom Energus holds personal data.

2.9 **Personal Data** is defined as data which relate to a living individual who can be identified or identifiable person (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, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;

- from those data, or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

and includes an expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of that individual.

2.10 **Special categories of data** refers to personal data revealing; racial or ethnic origins; political opinions, religious or philosophical beliefs; trade-union membership, genetic data, biometric data, data concerning health; sex life.

2.11 **Subject Access Request** is a written request from an individual to access any personal data that Energus holds about him/her. He/She also has the right to request the correction of any such data that is found to be incorrect.

3 Policy

3.1 The GDPR provides six principles to be adhered to in the processing of personal data. This is achieved by Energus by implementing appropriate rules and procedures. **ALL** Energus employees, contractors and consultants are therefore responsible for ensuring that these rules and procedures are followed. The objectives of the rules and procedures are to ensure that the six principles will be complied with and that all personal data is:

- processed lawfully and fairly in a transparent manner;

- collected for specified, explicit legitimate purposes and not further processed in a matter incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes;
- accurate and where necessary kept up-to-date;
- kept in a form which permits identification for no longer than is necessary for the specified purpose; and
- kept secure subject to appropriate technical and organisational measures against unauthorised or unlawful processing, accidental loss or destruction.

3.2 Under the terms of the GDPR, processing of data includes any activity to do with the data involved. All employees or other individuals who have access to, or who utilise, personal data, have a responsibility to exercise care in the treatment of that data and to ensure that such information is not disclosed to any unauthorised third party. Examples of personal data could include address lists and contact details as well as individual files. Any processing of such information must be done in accordance with Energus rules and procedures.

3.3 Additionally, in order to comply with the first principle, at least one of the following conditions must also be met;

- the subject has given his/her explicit consent to the processing (such consent must be recorded);
- the processing is necessary for the performance of a contract with the subject;
- processing is required under a legal obligation;
- processing is necessary to protect the vital interests (essential for the life) of the subject or another person;
- processing is necessary for the performance of a task carried out in the public interest;
- processing is necessary to pursue the legitimate interests of the Data Controller or third parties (unless it could prejudice the interests of the subject or would constitute processing carried out by a public authority in the performance of their tasks).

3.4 **Special Category (sensitive) Data**

If the personal data is deemed to be sensitive by the criteria described in 2.10, then additional conditions apply to its processing. Essentially, the explicit consent of the individual will usually have to be obtained before the data is processed unless the data controller can prove the processing is based on one of the following criteria;

- Compliance with employment law and obligations;
- To protect vital interests (essential for the life) of the data subject;
- The data subject has deliberately made the information public;
- To comply with legal obligations (establishing or defending legal rights);
- Processing is necessary for the establishment, exercise or defence of legal claims;
- Processing is necessary for the reasons of substantial public interest;
- Occupational medicine, provision of health or social care or treatment;
- Public health;
- Scientific or historical research or statistical purposes.

If you cannot justify the processing and holding of sensitive data, for one of the above reasons you must reconsider whether you should be gathering or holding that data at all. If the data needs to be held you must then obtain the explicit written consent from the data subject to ensure compliance (records of consent must be maintained to cover the entirety of the time and the data is held/processed).

If you do not have a lawful basis to justify holding/processing this category of data, you must remove the data from your records.

3.5 **Access rights**

Data subjects have the right to access personal data that Energus holds about them. Such a request is called a subject access request (SAR) and procedure ENG-IMP04 refers to the process that has to be followed. However, in summary, requests must be;

- processed by the DPO or suitably trained deputy;
- confirmed that the data subjects are who they say they are and have a right of access to the information;
- checked to ensure that any third party data subject's rights are not overlooked;
- respond to requested without undue delay and in any event within one month of receipt;
- recorded accurately.

3.6 It is also possible that Energus may receive a request from a data subject to erase personal data, rectify inaccurate data, restrict/cease or not begin processing personal data. All such requests or notices must be referred to the DPO and responded to either by;

- agreeing to comply with the request; or
- giving the reasons why the request is regarded as unjustified, either wholly or in part.

3.7 **Privacy Impact Assessments**

Privacy Impact Assessments (PIAs) are a tool that you can use to identify and reduced the privacy risks of projects. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help you design more efficient and effective processes for handling personal data.

A PIA should be carried out whenever a "new" project/process involving the use of personal information is being considered/initiated, especially if this involves the use of technology or third party processors e.g. new IT systems or contractors conducting work involving the processing of personal data.

The Energus DPO should be consulted. A template PIA form should be used to capture the process.

3.8 **CCTV**

Finally Energus operates a number of CCTV cameras in order to assist with security for its community and property. If any member of staff, consultant or contractor has any queries concerning the operation of these systems, he/she should contact the DPO or General Manager.

4 Documentation

- Records of subject access requests (Retained for 5 years)
- Records of communications resulting in an action to cease processing personal data (Retained for 5 years)
- CCTV records (Retained for 30 days unless otherwise required for longer as identified by the DPO and/or General Manager