Information Handling & Data Security Policy

1 Introduction

To support GCs and their teams (our "Champions") grow their impact and take energetic climate leadership, Lawyers For Net Zero (LNZ) collects, collates and analyses business and personal data from its Champions, potential Champions and people involved in our Champions' businesses, business partners, associates and business contacts. Data Subjects are the people or companies about whom we store data. This information needs to be treated carefully to ensure appropriate confidentiality is maintained.

This document describes the information security operating principles to be adopted by LNZ and people working for and volunteering with LNZ. These principles are aimed at providing appropriate data security for a small organisation and compliance with EU Directive on General Data Protection Regulations (GDPR) that came into force on 25 May 2018.

LNZ has a privacy conscious culture. We do not use cookies to collect personal data on individuals or companies and will not share (or sell) any individual's or company's information without their permission.

2 How we collect and use personal data

In the normal course of business, routine contacts with Champions and people involved in the Champion's business, suppliers, business partners and others will be collected to facilitate ongoing communication. This includes business contact data such as name, role, telephone numbers and email addresses. LNZ will not seek formal permission to store this business contact data but recognises its sensitivity as described below.

During formal discussions and contracting with Champions, potential Champions, business partners and associates LNZ will collect and process data, both personal and business related, in order that LNZ can provide services in a professional manner.

Data may also be collected in meeting notes, personal objectives, answers to questionnaires, discussions at meetings and workshops and meeting and workshop slides and outputs.

We will only use your personal data as permitted by the law allows us to which includes where it is necessary for our legitimate interests, where we need to comply with a legal or regulatory obligation & where we need to perform a contract with you.

3 Information types

Four classes of information are envisaged:

1. **Business contact data** - general contact data as described above for business communication
2. **Personal contact data –** personal contact details that allow an individual to be identified outside of work e.g. personal telephone number or home address
3. **Sensitive Personal data**. – in provision of services, sensitive personal data may become known to LNZ personnel. As defined under the Data Protection Act 1998 this includes racial or ethnic origin, political opinions, religious or similar beliefs and/or physical or mental health or condition,
4. **Sensitive Company data**. This is limited to information that is not in the public domain or easily deduced from information within the public domain. This includes strategic intent, information on organisation structure, commercial position, potential staff moves, workshop inputs and outputs, intellectual property etc.

4 Information treatment

The above information classes will be treated separately as follows.

Business contact data and personal contact data

This information is primarily contained in contacts databases, emails and appointment calendars. LNZ will use externally hosted email, contacts and calendar services. A professional, established application with active security oversight and updating will be utilised. The service provider is expected to comply with all relevant EE directives and standards in providing security of the data with respect to its services.

Where there is a reasonable expectation that introducing one person to another will be beneficial, LNZ will request permission to share contact email and other contact details with the other party.

Contact data is stored by LNZ personnel as long as it is considered useful for normal business needs.

Sensitive Personal and Company Data

Electronic versions of data will be stored on the internal LNZ network. Any paper copies or hand-written notes will be stored securely

Such data will be shared only with Data Subjects and others whom they have specified.

LNZ will always request a Champion's permission before using their feedback in any testimonial or case study.

LNZ personnel work remotely accessing electronic data via the LNZ network on suitably secure equipment.

No later than seven years after a programme or piece of advisory work is completed, all paper versions will be shredded and electronic copies deleted.

5 Data Subjects Rights

Date Subjects have various statutory rights. How we handle these is covered below:

The Right of Access – An individual can seek to obtain confirmation as to whether personal data concerning them is being processed by LNZ, where and for what purpose. Subjects also have the right to be provided with a copy of that personal data free of charge.

The Right to be Forgotten – All data including the classifications above are normally stored for a maximum of seven years. Should an individual request that data is destroyed sooner, then all sensitive personal data will be deleted as soon as possible. Note that LNZ will not delete data that shows that a commercial arrangement has been in place. This includes meeting dates, invoices etc. and data that is required for legal and tax purposes. There are several exceptions to the automatic deletion of data upon request:

a. If the provision of services is still ongoing, then suitable service termination arrangements are to be complete first.
b. If there is any dispute or ongoing action with the individual or organisation any information deemed by LNZ to be materially relevant will be held until such dispute is resolved.

The Right to Rectification – An individual can seek to have personal data held on them corrected without undue delay where the data concerning them is inaccurate.

The Right to Restriction – An individual can seek to restrict processing of the personal data held on them, subject to certain conditions. In LNZ this is likely to be associated with an end to the services provided and the conditions under "Right to be forgotten" would apply.

The Right to Object to Processing – An individual can object to processing personal data held on them.

The Right to Portability – An individual can receive the personal data concerning them in a "structured, commonly used and machine-readable format".

The Right to Lodge a Complaint with a Data Protection Regulator – An individual can make a complaint before a regulator about data protection issues concerning them.

6 Technical Considerations

Website
The LNZ website will not hold any sensitive company data. Personal data such as a name on a testimonial or case study will only be presented with the individual's explicit agreement.

Wireless Networks
All internal LNZ wireless networks will use WPA encryption and be password protected with a strong password.

PCs.
All PCs used by LNZ personnel will be password protected. Antivirus and firewalls will be installed and security updates applied as they become available.

Portable Devices
Portable devices such as phones and laptops must be password protected.

Cloud storage
The availability of reliable and secure cloud storage means that it LNZ may use cloud storage for documents and files that need to be accessed remotely from the office by clients or LNZ personnel.

Storage and File Structures
File structures are to be designed to make it easy to locate, separate and manage sensitive information.

7 Security Breaches

If any LNZ employee, volunteer, associate or supplier becomes aware of leakage or breach of security on sensitive information, or of systemic loss of personal data (e.g. mail service provider has suffered a theft of personal data), then the data controller must ensure that relevant clients or individuals are contacted as soon as possible advising of the breach, the data lost and an action plan agreed.

8 Approvals & reviews

This document has been approved by our CEO, Adam Woodhall. It will be reviewed when material changes are required.