Mechanical & Electrical Contractors

GDPR Policy

Introduction

LJJ is committed to conducting its business in accordance with all applicable Data Protection laws and regulations and in line with the highest standards of ethical conduct. This policy puts into place the expected behaviours of LJJ Employees in relation to the collection, use, retention, transfer, disclosure and destruction of any Personal Data belonging to a LJJ Contact (i.e. the Data Subject).

Personal Data is any information which could relate to an individual person identified or Identifiable Data. An organisation that handles Personal Data and makes decisions about its use is known as a Data Controller. LJJ could be classed as a Data Controller, therefore we are responsible for ensuring compliance with the Data Protection requirements outlined in this policy. Non-compliance may lead to complaints, regulatory action, fines and/or reputational damage for LJJ Contractors as a whole.
Any breach of this policy will be taken seriously and may result in disciplinary action.
This policy has been approved by all LJJ Directors.

LJJ as a business do not deal direct with individuals or the general public therefore we don't store any PII other than employees or previous employees of the business.

This Policy applies to three main areas of work within the company that hold a Data Subjects Personal data:

Section 1: Information Technology

Section 2: Accounting

Section 3: General

This should cover all processing and protection of personal data both in a physical and digital form within the company.

There are also some definitions that should be outlined that are noted in the policy:

Employee:

An individual who works part-time or full-time for LJJ under a contract of employment, and has recognised rights and duties.

Third Party/Sub-Contractor:

An external organisation with which LJJ conducts business and with implied permission and consent to have related personal data held and or processed by LJJ Ltd.

Personal Data:

Any information which could relate to an individual person identified or Identifiable Data.

Identifiable Person:

> Anyone who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location, a personal online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Controller:

> A 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.

Data Subject/Citizen:

> The identified or Identifiable Person to which the data refers.

LJJ has appointed Phil Rowe as the Data Protection Controller (DPC) who will ensure that all personal data is processed in compliance with the new GDPR legislation.

Section 1: Information Technology

This First section of the policy will focus on how GDPR will impact the processing of Personal Data in the IT department of LJJ.

Names, Passwords, Usernames, and E-mail Addresses:

When an Employee starts with LJJ they are granted a Username Password and E-mail Address these are generated under the implied consent to use the Data Subjects full name in the creation process for the user name and e-mail address. Passwords are completely randomly generated and have no relation the individual Data Subject, however in some cases Data Subjects may have their passwords changed either by request or the Data Controller these changed passwords may contain Personal Data like the name of a significant other or place of residence this is not advised (in the case of a Data Breach) but permitted if requested with the permission of Data Subject.

LJJ Ltd will not be held responsible in the event of a data breach, loss or leak of Personal information held on Third Party Accounts created by the Data Subject using their designated LJJ E-mail Address, such as Dropbox and other file sharing websites.

Personal Data and Desktops/Laptops:

Desktops, Laptop and tablets issued by LJJ Ltd are to have as minimal Personal Data Stored on them as possible this is for many reason such as creating storage issues on smaller capacity machines, and also in the event of hardware failure like a broken hard-drive company resources could be wasted on trying to recover non-company related files. Leaving personal Data unattended is the second most common way for a Data Breach to occur next to Hacking and Malware, therefore it is one of LJJ Ltd priorities to make sure users take proper care of their company property and reduce the chance of a Data Breach in this way.

Whenever a Laptop or Desktop is returned to head office for reconfiguration be it because the Data Subject has left the company or is just receiving updated hardware all personal data of the previous user is completely

removed from the laptop to prevent an accidental breach of Personal Data. In the event of a departure of a Data user from the company the Laptop Tablet or Desktop must be returned to Head Office for proper reconfiguration to comply with GDPR legislation.

Right to be forgotten:

A large Part of GDPR Policy is the right to be forgotten, there for LJJ Contractors will act appropriately when asked to erase non-relevant data on a Data Subject that we hold personal data on. (Job expiry will of course, be a factor on deciding what data is relevant.)

Data Breach:

Data Breach *- A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.*

In the event of a Breach of Disclosure a reporting failure must be processed for example a data breach could be as simple as if a lot of internal E-mail addresses are CC'd instead of BCC'd this is a breach however it is more manageable and depending on the involved parties this could be overlooked; however, this could also apply if a intended internal e-mail is sent to an external source this less excusable. We have in place a countermeasure for cases like this in our e-mail signature that reads as follows:

"*The information contained in this message may be confidential and/or legally privileged. It is intended only for the persons named as addressees. The dissemination, distribution, copying or disclosure of this message or its contents is prohibited unless authorised by the sender".*

If received in error please contact the sender or telephone quoting the name of the sender and destroy the message immediately.

Unless expressly stated in the body of this message no contractual commitment has been entered into by the sender by virtue of this communication.

Any views expressed by an individual within this email do not necessarily reflect the views of the Company. We do not accept responsibility for any viruses and you should therefore scan the message, body, and any attachments prior to opening."

How to Protect your Personal Data

Laptops and Portable Devices:

All laptops and portable devices that hold data containing personal information must be protected with a suitable encryption program.
Ensure your laptop is locked (password protect) when left unattended, even for short periods of time.
When travelling in a car, make sure the laptop is out of site, preferably in the boot.
If you have to leave your laptop in an unattended vehicle at any time, put it in the boot and ensure all doors are locked and any alarm set.
Never leave laptops or portable devices in your vehicle overnight.
Do not leave laptops or portable devices unattended in restaurants or bars, or any other venue.

When travelling on public transport, keep it with you at all times, do not leave it in luggage racks or even on the floor alongside you.

Data Security and Storage:

Store as little personal data as possible on your computer or laptop; only keep those files that are essential. Data received on disk or memory stick should be saved to the relevant file on the server or public folder. The disk or memory stick should then be securely returned or processed for safe storage or disposal.

Always lock (password protect) your computer or laptop when left unattended; this is especially important when using your laptop away from the office.

Passwords:

Do not use passwords that are easy to guess. Make sure all of your passwords contains a mix of both upper and lower-case letters and preferably contain some numbers. Ideally passwords should be 8 characters or more in length.

Protect Your Password:

- Do not give out your password
- Do not write your password somewhere on your laptop
- Do not keep it written on something stored in the laptop case
- If you believe you password has been compromised please have it changed immediately
- When creating accounts not controlled by the company avoid the following passwords:

1. 123456
2. 123456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321

Section 2: Accounts

This Second Section will describe how the Accounts department uses Personal Data.

Overall:

All users have individual passwords for Windows, Sage Accounts and Sage Payroll

Log of passwords is kept on Steve Baines Personal Network Drive

Banking:

HSBCnett holds all payments on all the accounts below for 6 months (this obviously includes individual bank details etc.), access to the bank is on an access level required basis with individual log ins

Users have access to only certain accounts and this is protected by a username and password – then an access code is required using a device that itself is individually pin protected.

HSBC Current Access is as follows:

Steve Baines – Full access to all accounts, no restrictions other than authorisation and user setup

Lee Rennison – Full access to all accounts, no restrictions and payment authorisation/user setup

Ian Rennison – Full access to all accounts, no restrictions and payment authorisation (for LJJ Ltd only)

Jane Kelsey – LJJ Ltd only with restrictions

Joe Secret – LJJ Ltd only with viewing only

Anthony Reed – LJJ Ltd with viewing only

Lauren Appleby – Clear Climate only with restrictions

Sarah McCulloch – Martin Design only with restrictions

LJJ Payroll:

Monthly

Starter Letters/Contracts issued from Directors to Lee/Steve B via email, Emails to be deleted by SB/LR once processed Directors delete from Sent Box immediately.

Start Letters are kept in Lee Rennison's Office locked away in filing cabinet.

Other personal information including Starter Form, HMRC, Holiday and Sickness, Training records are kept downstairs locked in filing cabinet that only Alyson Andrews has Access to. Central Office and The High Wycombe Office utilise a secure folder structure on the network drive that has strict permission security to hand over information to Alyson.

Access to monthly payroll on Sage – Steve B only – Password Protected

Paper files for two years are to be kept in Steve Baines office in locked filing cabinet

CSV files are to be deleted historically and then each period they are deleted once uploaded and sent to the bank

BAS Report is no longer printed

Mechanical & Electrical Contractors

Weekly:

Current Employees – all their personal information is locked away in filing cabinet in accounts office (Jane Kelsey holds the key, access given to Josephine McKee for filing), starter forms may have been emailed they are then promptly deleted.

New Employees, request for contract made by Directors to Jane Kelsey, Jane will raise the contract, issue in post and once returned will be filed away in cabinet once setup on Payroll.

All personal information including tax information, starter information (which may contain an individual's personal bank details and/or Passport) sickness and holiday records are filed in a secure cabinet handled by Steve Baines/Jane Kelsey. Some information is held for training purposes and is dealt with by Gemma Cann.

Paper files are no longer kept for each Payroll Processing period, Payment summaries, Payslips and Timesheets etc are now digitally scanned via pdf into the Weekly Wages folder on Admin/Accounts Only - which is permission locked for high level access.

Access to weekly payroll on Sage – Steve B, Jane Kelsey only – Individually Password Protected.

CSV files are to be deleted and then each period they are deleted once uploaded and sent to the bank.

BACS report is no longer printed nor Scanned in as above is it is not required.

Suppliers/Sub Contractors:

All suppliers since the company formed still have their account on Sage Accounts (with their bank details etc.) Sage Accounts is protected by individual passwords for each user however.

Suppliers bank details are normally on their invoice or statement as well, paper records for last 2 years are kept in the accounts department and then are archived in the loft after that.

Bank details/other supplier information will be on emails, especially sub-contractors.

Mechanical & Electrical Contractors

Section 3: General

Admin

What type of information is collected from you:

The personal data we collect may include:

• Name	Stored in locked filing cabinet / locked index box
• Address	Stored in locked filing cabinet / locked index box
• Private Email address	Stored in locked filing cabinet
• Business Email address	Stored on server
• Telephone number	Stored in locked filing cabinet / locked index box
• Work mobile number	Stored on server
• Personal mobile number	Stored in locked filing cabinet / locked index box
• Date of birth	Stored in locked filing cabinet / locked index box
• Medical details	Stored in locked filing cabinet
• Training record	Stored on server
• Next of kin	Stored in locked filing cabinet
• NI number	Stored in locked filing cabinet / locked index box
• CV and associated certificates	Stored in locked filing cabinet
• Training records	Stored on server
• Copy of Driving licence	Stored in locked filing cabinet
• Copy of Passport (Right to work in the UK)	Stored in locked filing cabinet
• Confidential letters/documents to and from Staff member and LJJ	Stored in locked filing cabinet / locked index box

How is your information used:

- Processing of financial matters including wages/salaries.
- Details to third parties such as H&S organisation and training providers.
- Displayed on the LJJ Limited Web site.
- Presentation documents.

Upon Company departure the following information is held:

Your Payroll information including personal information will be held on Sage Payroll until end of the tax year (April), then your employee record will be permanently deleted from Sage Payroll.

Payroll processing files will be kept for 2 years in a locked filing cabinet then they will be transferred to a secure storage facility for an additional 4 years. Thereafter the processing files will be incinerated.

Starter forms, training records, holiday records, tax information etc will be kept in a locked filing cabinet indefinitely unless a special request under GDPR legislation is made.

CCTV Records:

CCTV footage of individuals and licence plates are held by ABCA and data is held as their GDPR policy.

Mechanical & Electrical Contractors

The named person below has overall responsibility for dealing with all issues relating to this GDPR policy and will periodically review the statement in accordance with the relevant provisions.

Name: Ian R. Rennison Position: Managing Director

Signed:  Date: June 2018