Life Compass Consulting Ltd

GDPR Policy

1st June 2018

Data Controller & Data Processor

The data controller and data processor are Life Compass Consulting Ltd

Data Processing Summary Statement

Business Customers- we collect data on our business customers to deliver the work we have been contracted to do. We collect names, addresses, emails, location details and notes relating to business discussions. It is a requirement that we communicate regularly with our customers so that we can fulfil their requirements. We send service reminders, details of new offerings, emails to define the detailed spec of the work and other important business information on the basis of Contractual Obligation or Legitimate Business Interest. We also invoice and chase invoices on the grounds of legitimate interest.

With our business customers, we mail and email them on the basis of legitimate business interest. Because they are customers, and have been presented with the opportunity to opt out, on every communication, and when the data was collected, we do this under PECR soft opt-in.

Communications to business customers therefore include:

1) Emails, letters and phone calls, required to sell the product
2) Periodic email newsletter to customers, informing them of developments in the market, and services we offer.

Business Prospecting- we source data on potential customers, both individuals and companies, and prospect to them via direct mail, email, newsletter and phone calls. We communicate to them on the grounds of legitimate business interest- it is in our interest to develop relationships with this audience in order to sell them our services in the future. They have the opportunity to opt out.

Data Security

Data is stored in the most secure way that we can, which allows us to deliver on contracts. The data we hold, being email addresses or Business to Business data, is very low risk.

All laptops are encrypted and password protected and all company phones have pin numbers and are connected by 'find my phone' allowing the data on them to be cleansed.

Online storage- we use Microsoft OneDrive cloud storage and emails are sent through Godaddy. Our due diligence shows that these organisations adhere to the standards required by GDPR.

Data Breech Process

We have the following obligations:

- To inform the Information Commissioner if there is a serious breech of data security within 72 hours of the breech occurring
- To inform the data subject if there is likely to be any harm arising from that breech

Our process is as follows:

1) Data breech is discovered. The breech is noted in the log book, time and dated, noting which data has been affected. The extent, and seriousness of the breech is assessed, including the potential harm to the data subject.
2) For a serious breech, the data controller will inform the ICO on the working day of the breech being discovered.
3) Within 1 working day, if the initial assessment concluded that there is a potential harm to the data subject, the data controller will inform the data subject (customer). For the sake of clarity, name, address and contact details are, in our view, unlikely to give rise to harm, while credit card and bank details are highly likely to give rise to harm.
4) Within 1 month of the data breech, the data controller will carry out a review of the data protection policy, and put in place steps to mitigate risks of subsequent breeches.

Data Table

Segments	**Type**	**Sources**	**Storage**	**Process**	**Legal basis for the process**
Customers	Private individuals	Direct contact from customer	Stored on password-protected, encrypted laptop and 'cloud'	Delivery of job process. Reminder for follow up work.	Legal & contractual obligations. Legitimate business interest
Customers	Businesses & Organisations	Direct contact			
Business prospects	Businesses & Organisations	Research Referrals		Email & phone marketing	Legitimate business interest
Web data-analytics	Private individuals	Google web analytics	Stored on google systems, accessible vie gmail password. We do not track or store IP address	Analysis of traffic, sources, by general demographics and geography. There is no process to identify individual persons	Legitimate business interest

Privacy Impact Assessment

Risk	Impact 1-5	Likelihood	Response	Action	Owner
Laptop lost	2	3	None	Encrypt laptop	Data controller
Cloud provider hacked	3	1	None	Ensure sensitive data is not captured	Data controller
Phone lost	2	3	None	Password protect phone. Use 'find my phone' and cleanse data if lost	Data controller
Notebooks or other paperwork lost	1	3	None	None	NA

Summary statement

All data processing operations carried out by Life Compass Consulting Ltd have been assessed to be covered by 'legal and contractual obligations' or 'legitimate business interest', and our due diligence shows that the controls adhere to the standards required by GDPR.

Signed by: Lisa C Cox

Role: Director

Dated: 1st June 2018