Making Business Sense

Cebr Privacy and Data Security Policy

Introduction

Cebr takes security of data very seriously**.** We show this in a range of ways.

1) Cebr has the Cyber Essentials certification. This certification is renewed annually following a reassessment of Cebr's cyber security processes.
2) Cebr staff are contractually committed to confidentiality.
3) Cebr ensures staff are adequately trained in the essentials of data security with the training updated annually.
4) We only work with third party suppliers such as IT suppliers whose data security practices at least match our own.

Details

This document sets out how Cebr looks after the security of data it collects and holds. This is described for all data in general, followed by a section on how Cebr is compliant with GDPR in relation to personal data and a section on the additional steps we take to protect sensitive data.

Storing information

Information which is submitted to Cebr is stored on our computers and backed up on a secure server located within the UK.

Security of client data, any other input data, work in progress and reports is arranged by saving it on our secure file server.

All Cebr staff have strong and regularly changed passwords for access to the server.

Where data is particularly sensitive we will additionally password protect the specific files containing it, so that only those working on the specific project have access.

Remote access to the Cebr secure network is only permitted using the secure VPN on company laptops.

Our operational risk policy details clear rules for production, transmission and storage of documentation: Records are kept electronically, filed by client for all contractual papers, data, work in progress and reports. Correspondence is filed electronically by project number. Drafts of reports are numbered, dated, and kept with final reports in a separate report file.

Survey data will be retained or deleted at the end of a project depending on the agreement with the client for whom we are working.

File Server, Back-up and Security and catastrophe provisions.

Our site is alarm-protected and our servers are contained in a locked storage unit.
Our file server is backed up daily and stored offsite in a secure datacentre. These backups are encrypted in transit and at rest. This enables complete file server data recovery in the event of hardware failure or other significant on-site IT disruption.

Cyber-attack protection

Cebr has Cyber Essentials certification which we update every year. All our computers run anti-virus software that is updated daily. Staff are reminded regularly about good housekeeping, and the need for strong passwords.

Special considerations for personal data in line with GDPR

All personal data is handled fairly and lawfully in accordance with individuals' rights and the principles of GDPR, and staff are trained regularly in these.

If you require a full copy of our Data Protection Policy, (which covers personal data) please email dataprotectionmanager@cebr.com to request one. All legitimate requests will be granted.

Personal Data

Key elements of our policy towards personal data are set out below:

Where do we collect personal information?
We may collect personal information in a number of ways, including:

- When you send us data by email: your email address may be personal data.
- When we collect it as you use our website- specifically if you wish to download a report, or apply for a post, make an enquiry, or request a free trial of our Prospects Service.
- When we contract with you or your organisation and continue in contact during a project.
- When you agree to receive our reports or press information.

How will we use your personal information?
Personal information collected and processed by us may be used, for the following purposes:

- To reply to your enquiry or request.
- If you supplied it in connection with a report download, to update you on what Cebr can provide where you have consented to receive such communications from us.
- To communicate over the legitimate conduct of a contract.

We will not share your information: It is not our policy to sell or pass on your data to other organisations to use for their own purposes.

Any personal information you supply to us will be retained for no longer than necessary and will be removed from our systems or securely disposed of in accordance with the requirements of our Data Protection Policy.

If you send in a survey response, we will only use the response itself in such a way that the individual response and respondent cannot be identified.

Security
We have security measures in place to protect against the loss, misuse and alteration of personal information under our control. Whilst we cannot ensure or guarantee that loss, misuse or alteration of information will not occur, we will use standard industry methods to prevent this.

Storing data securely

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it.
- Printed data will be shredded when it is no longer needed.
- Data stored on a computer is protected by strong passwords that are changed regularly.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used.
- The DPM must approve any cloud used to store data.
- Servers containing personal data are kept in a secure location, away from general office space.
- Data is regularly backed up in line with the company's backup procedures.
- All servers containing sensitive data must be approved and protected by security software.
- All possible technical measures must be put in place to keep data secure.

Data retention

We do not retain personal data for longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Sensitive data (e.g. commercially sensitive)

We often work with data that is especially sensitive for a range of reasons (e.g. commercially sensitive data).

If this is the case we apply two additional data security procedures:

- Sensitive data is stored in password protected files so that only the key staff using the data have access to it.

- Sensitive data is routinely deleted at the end of each project unless there is a specific agreement with both the client and the data provider to retain the data.

IPMcW
December 2020