Data Protection Policy

Context and overview

Key details

- Policy prepared by: Director
- Approved by GVE Board on: May 22 2018
- Policy became operational on: May 25 2018
- Next review date: August 17 2021

Introduction

GVE Commercial Solutions Limited ("GVE") needs to gather and use certain information about individuals.

'Individuals' can include employees, working sub-consultants, advisory consultants and other people the business has a relationship with or may need to contact.

This policy describes how this personal data is collected, handled and stored to meet GVE's data protection standards and to comply with the law.

Why this policy exists

This data protection policy ensures that GVE, its employees, any working sub-consultants, advisory consultants and relevant third parties comply with data protection laws and follow good practices, protect the rights of individuals, is open about how it/they store and process individuals' personal data and protects itself/themselves from the risks of a serious data breach.

People, risks and responsibilities

Policy scope

This policy applies to all employees of GVE, all working sub-consultants, advisory consultants and relevant third parties.

It applies to all personal data that GVE holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses

- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect GVE from some serious data security risks, including:

- **Breaches of confidentiality,** for instance information being given out inappropriately,
- **Failing to offer choice,** for instance all individuals will be free to choose how GVE uses data relating to them,
- **Reputational damage,** for instance GVE could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone in GVE, including its working sub-consultants, advisory consultants and relevant third parties has some responsibility for ensuring data is collected, stored and handled appropriately.

General guidelines

- The only people able to access personal data covered by this policy will be those who need it for GVE business activities,
- Personal data will not be shared informally,
- GVE employees, its working sub-consultants, advisory consultants and relevant third parties must keep all personal data secure by taking sensible and proportionate precautions,
- In particular, strong passwords must be used and they should never be shared,
- Personal data will not be disclosed to unauthorized people, either within GVE or externally,
- Personal data will be regularly reviewed and updated if it is found to be out of date. If it is no longer required it will be deleted and securely destroyed,
- GVE offices must always be locked and alarmed when not in use and computers always locked in a drawer or cupboard,

- GVE employees who store and process sensitive personal data and who take that computer away from the office must have a suitable encryption key fitted to their computer,
- GVE employees will request help if they are unsure about any aspect of data protection,
- Working consultants, advisory consultants and relevant third parties shall carry on their related business with GVE with these guidelines, and more generally this data protection policy in mind, and shall, unless disproportionally difficult to do so, abide by its rules, guidelines and permissions.

Data storage

These guidelines describe how and where data will be safely stored.

Where and when data is stored on paper it will be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been stored on paper for some reason:

- When not required the paper or files will be kept in a locked drawer or filing cabinet,
- Paper or files shall not be left unattended where unauthorized people could see them, copy them or take them, for instance on a printer,
- Paper will be shredded and disposed of securely when no longer required.

Where and when personal data is stored electronically, it will be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Personal data will be protected by strong passwords that are changed regularly and never shared,
- If personal data is stored on removable media (like a CD or DVD) these will be kept locked away securely when not in used,
- Personal data will only be stored on designated drives and servers and will only be uploaded to GVE approved secure cloud computing services, or in the case of working sub-consultants, advisory consultants or relevant third parties third own similarly protected service.
- Personal data will be backed up frequently. Those backups will be tested regularly, in line with good quality and robust backup procedures,

- Personal data should never, inappropriately, be saved directly to laptops or other mobile devices,
- All computers containing personal data will be protected by approved security software and an appropriate firewall.

Data use

- When working with personal data computer screens shall be locked when left unattended,
- Personal data must be encrypted before being transferred electronically,
- GVE employees, working sub-consultants, advisory consultants and relevant third parties shall not unnecessarily save copies of personal data to their own computers.

Data accuracy

The law requires GVE to take reasonable steps to ensure personal data is kept reasonably accurate, relevant and up to date. Data accuracy will be reviewed at least annually and the results recorded in the minutes of GVE's Board meetings.

Subject access requests

All individuals who are the subject of personal data usage, held by GVE, are entitled to:

- Ask what information GVE holds about them and for what purpose,
- Ask how to gain access to it,
- Be informed on how to keep it up to date,
- Be informed on how GVE is meeting its data protection obligations.

If an individual contacts GVE requesting this information this will be called a subject access request.

Subject access requests from individuals will be made by email, addressed to the **Data Controller** (one of the GVE directors) at **jdear@gvecs.co.uk.**

Individuals will be charged £10 per subject access request unless expressly waived by one of GVE's directors. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances the Data Protection Act allows personal data to be disclosed to law enforcement agencies that request it without the consent of the data subject.

Under these circumstances GVE will disclose the requested data. However, the data controller will ensure the request is legitimate and will seek legal guidance if and when necessary.