BJH Data Protection Policy

Updated 24.06.2020

Key details:

- Policy prepared by: Mrs Stacey Lea Holleron

  (Director)
- Approved by board/ management on: 24.06.2020
- Policy became operational on: 24.06.2020
- Next review date: 23.06.2021

Introduction:

BJH CONTRACTS UK LTD need to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees, sub-contractors and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the Company's data protection standards – and to comply with the law.

Why this policy exists:

This data protection policy ensures that BJH CONTRACTS UK LTD:

- Complies with data protection law and follow good practice
- Protects the rights of staff, customers, partners and sub-contractors
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection Law:

The data protection Act 1998 describes how organisations – including BJH CONTRACTS UK LTD – must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The data protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and unlawfully

2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, Risks and Responsibilities

Policy Scope

This policy applies to:

- The head office of BJH CONRACTS UK LTD
- All branches of BJH CONTRACTS UK LTD
- All staff of BJH CONTRACTS UK LTD
- All contractors, suppliers and other people working on behalf of BJH CONTRACTS UK LTD

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Emergency contact details
- …plus any other information relating to individuals

Data Protection Risks

This policy helps to protect BJH CONTRACTS UK LTD from some very real data security risks, including:

- **Breaches of confidentiality**. For instance, information being given out inappropriately

- **Failing to offer choice.** For instance, all individuals should be free to choose how the Company uses data relating to them and request any data being held with regards to them at any time. Also, individuals have the right to update incorrect data and/or have data erased.

- **Reputational Damage.** For instance, the Company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with BJH CONTRACTS UK LTD has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

- The board of Directors is ultimately responsible for ensuring that BJH CONTRACTS UK LTD meets its legal obligations.

- The Data Protection Officer – Mrs Stacey Lea Holleron – is responsible for:

a) Keeping the board updated about data protection responsibilities, risks and issues

b) Reviewing all data protection procedures and related policies, in line with an agreed schedule

c) Arranging data protection training and advice for the people covered by this policy.

d) Handling data protection questions from staff and anyone else covered by this policy.

e) Dealing with requests from individuals to see the data BJH CONTRACTS UK LTD holds about them (also called 'subject access requests').

f) Checking and approving any contracts or agreements with third parties that may handle the Company's sensitive data.

g) Ensuring all systems, services and equipment used for storing data meets acceptable security standards.

h) Performing regular checks and scans to ensure security hardware and software is functioning properly.

i) Evaluating any third-party services, the Company is considering using to store or process data. For instance; cloud computing services.

j) Approving any data protection statements attached to communications such as emails and letters

k) Addressing any data protection queries from journalists or media outlets like newspapers

l) Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General Staff Guidelines

- The only people to access data covered by this policy should be those who **need it for their work**.

- Data **should not be shared informally.** When access to confidential information is required, employees can request it from a Senior member of staff or line manager.
- **BJH CONTRACTS UK LTD will provide training** to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, **strong passwords must be used** and they should never be shared.
- Personal data **should not be disclosed** to unauthorised people, either within the Company or externally.
- Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.
- Employees should request help from the Data protection officer if they are unsure about any aspect of data protection.

Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Data Controller.

When data is **stored on paper**, it should be kept in a secure place where unauthorised people cannot see it.

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

- When not required, the paper of files should be kept in a **locked drawer or filing cabinet.**
- Employees should make sure paper and printouts are **not left where unauthorised people could see them,** like on a printer.
- **Data printouts should be shredded** and disposed of when no longer required.

When data **is stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers,** and should only be uploaded to an **approved cloud computing service.**
- Servers containing personal data should be **sited in a secure location**, away from general office space.

- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the Company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets of smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall.**

Data Use

Personal data is of no value to BJH CONTRACTS UK LTD unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Data will only be shared with third parties if agreed by the individual in writing.
- Once the use for data has been completed, data should be disposed of fully and appropriately.