Solihull BID Limited

DATA PROTECTION POLICY

Document Control

Organisation	Solihull BID Limited
Title	Data Protection Policy
Author	John Timms – Operations Manager, Solihull BID
Filename	DPP001
Owner	John Timms – Operations Manager, Solihull BID
Subject	Solihull BID Data Protection Policy
Protective Marking	None
Review Date	24th May 2018

Revision History

Revision Date	Version Number	Revised By	Description of Revision
15th May 2018	1	John Timms	First Edition

Document Approvals

This document requires the following approvals:

Job Title	Name	Date
Solihull BID Limited	BID Board of Directors	11th June 2018

1. Context and overview

Key details

- Policy prepared by: John Timms
- Approved by board / management on:
- Policy became operational on:
- Next review date:

Introduction

Solihull BID Ltd needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees 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 Solihull BID Ltd.

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

Data Protection Law

Anyone who handles personal information about individuals has a number of legal obligations to protect that information. The BID, its directors and staff handle such information, therefore the BID must comply with data legislation.

The Data Protection Act 1998 describes how organisations — including Solihull BID 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 1998 is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
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

The new General Data Protection Regulation (GDPR) sets out new principles. These are similar to the old principles, but with the important addition of a new accountability principle which holds the BID

to account for showing how it complies with the principles, for example by documenting the decisions it takes about a processing activity.

Article 5 of the GDPR requires that data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public; interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that "the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The GDPR Data Protection Policy details how the BID will seek to protect personal data and ensure that the BID Board of Directors and BID staff understand the rules governing their use of the personal data to which they have access in the course of their work.

2. People, risks and responsibilities

Policy scope

This policy applies to:

- The registered office and postal address of Solihull BID Ltd
- All staff and volunteers of Solihull BID Ltd
- All contractors, suppliers and other people working on behalf of Solihull BID 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;
- plus, any other personal information relating to individuals

Data protection risks

This policy helps to protect Solihull BID 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.
- Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities
Everyone who works for or with Solihull BID Ltd has some responsibility for ensuring data is collected, stored and handled appropriately.

Each person 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 Solihull BID Ltd meets its legal obligations.
- The data controller, John Timms, is responsible for:
  - Keeping the board updated about data protection responsibilities, risks and issues.
  - Reviewing all data protection procedures and related policies, in line with an agreed schedule.
  - Arranging data protection training and advice for the people covered by this policy.
  - Handling data protection questions from staff and anyone else covered by this policy.
  - Dealing with requests from individuals to see the data Solihull BID holds about them (also called 'subject access requests').
  - Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
  - Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
  - Performing regular checks and scans to ensure security hardware and software is functioning properly.
  - Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.
  - Approving any data protection statements attached to communications such as emails and letters.
  - Addressing any data protection queries from journalists or media outlets like newspapers.
  - Where necessary, working with other staff to ensure marketing initiatives abide by data protection and GDPR principles.

3. General staff guidelines

- The only people able 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 their line managers.
- Solihull BID 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 their line manager or the data controller if they are unsure about any aspect of data protection.

4. Data storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the BID Director or 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 or 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 securely 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 memory stick, external hard drive, CD or DVD), these should be kept locked away securely when not being used. Data should be deleted from the memory stick after use.
- Data should only be stored on designated drives or servers and should only be uploaded to an approved cloud computing services.
- Drives 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 (every 4 weeks).
- Data should never be saved directly to mobile devices like tablets or smart phones.
- All servers, drives and laptops containing data should be protected by approved security software and a firewall.

5. Data Use

Personal data is of no value to Solihull BID 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.
- Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.
- Data must be encrypted before being transferred electronically.
- Personal data should never be transferred outside of the European Economic Area.
- Employees should not save copies of personal data to their own computers.
- Always access and update the central copy of any data.

6. Data Accuracy

The law requires Solihull BID to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Solihull BID should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Solihull BID will make it easy for data subjects to update the information Solihull BID holds about them. For instance, via the Solihull BID website and the info@solihullbid.co.uk email account.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the BID Director's responsibility to ensure BID Levy database and other marketing databases are checked for accuracy every six months.

7. Subject Access Requests

All individuals who are the subject of personal data held by Solihul BID are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If individuals contact the BID requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at datacontroller@solihullbid.co.uk. The data controller can supply a standard request form, although individuals do not have to use this. Individuals will not be charged under this request under GDPR. The request will be emailed to all the BID Board of Directors, where the request will be logged. The data controller will provide the relevant data within 21 working days.

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

8. Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Solihull BID will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the BID Board of Directors and from the appointed BID company's legal advisors where necessary. This type of disclosure would normally be in relation to any video footage of a crime related incident that was captured by a Town Host on their body worn camera.

9. Providing Information

Solihull BID aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the BID has privacy statements, setting out how data relating to individuals is used by the company.

A version of these statements is also available at www.solihullbid.com