Data Protection Policy

Bandicoot Limited

Introduction

We need to gather and use information about clients, suppliers, business contacts, associates, employees and potential clients.

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 Data Protection Act 1998 and the General Data Protection Regulations introduced on 25th May 2018.

This policy applies to:

- All employees of Bandicoot Limited;
- All contractors, suppliers and other people working on behalf of the Company.

This policy applies regardless of whether data is stored electronically or on paper.

Why this policy exists

This data protection policy ensures that the Company:

- Complies with data protection law and follow good practice;
- Protects the rights of staff, clients and associates;
- 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 is underpinned by eight 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 G.D.P.R. applies to all data that the Company holds relating to identifiable individuals. This can include:

- Names of individuals;
- Postal addresses;
- Email addresses;
- Telephone numbers.

The regulations place greater obligations on how organisations handle personal data.

Data protection risks

This policy helps to protect the Company from data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately;
- **Prosecution by the ICO.** For failing to protect an individual's personal data;
- **Reputational damage.** For instance, the Company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with the Company has some responsibility for ensuring data is collected, stored and handled in line with this policy and data protection principles it covers.

However, these people have key areas of responsibility:

- The **Company Directors** are responsible for ensuring that the Company meets its legal obligations.

- The **G.D.P.R. Co-ordinator, Anna Bowen,** is responsible for:

    - Keeping 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 we hold 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.

- The **Managing Director, Stuart Bowen,** is responsible for:

    - 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.

- The **Senior IT Technician, Tom Coley,** is responsible for:

    - Approving any data protection statements attached to communications such as emails and website policies/statements;
    - Working with other staff to ensure marketing initiatives abide by data protection principles.

Staff guidelines

The only people able to access data covered by this policy should be those who **need it for their work**. 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;
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line manager;
- Employees should undertake **training provided** by the Company to all employees to help them understand their responsibilities when handling data;
- Employees **should request help** from their line manager or the G.D.P.R. Co-ordinator 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 Managing Director or G.D.P.R. Co-ordinator.

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:

- 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 pen drives, CDs or external disks), 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 **a cloud computing service provider approved** by the Managing Director;
- 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 or 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 the Company 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**. In particular, care should be taken when sending personal data by email, as the recipient's server or computer may not be encrypted;
- Data must be **encrypted before being transferred electronically**. The Senior IT Technician can explain how to send data to trusted and technologically competent external contacts;
- 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.

Data accuracy

The law requires the Company to take reasonable steps to ensure data is kept accurate and up to date. 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 deleting a contact who has ceased trading;
- Data should be **updated as inaccuracies are discovered**. For instance, if a client can no longer be reached on their stored telephone number, it should be removed from the database;
- It is the Senior IT Technician's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject access requests

All individuals who are the subject of personal data held by the Company 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**.

Subject access requests from individuals should be made by email, addressed to the G.D.P.R. Co-ordinator at info@bandicoot.co.uk. The G.D.P.R. Co-ordinator will provide the relevant data within 30 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 without the consent of the data subject.

Under these circumstances, the Company will disclose requested data. However, the G.D.P.R. Co-ordinator will ensure the request is legitimate, seeking assistance from the Company's legal advisers where necessary.

Providing information

The Company 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.

The Company has a privacy notice, setting out how data relating to individuals is used by the Company. To view the privacy notice please see www.bandicoot.co.uk/privacy.

16th May 2018