GDPR Operational Data Protection Policy

Toucan Internet LLP
Issue 1.0

Introduction

Toucan Internet LLP needs to gather and use information about clients, suppliers, business contacts, associates, and potential clients.

This policy describes how this personal data must be collected, handled and stored to meet the Toucan Internet LLP'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 Partners of Toucan Internet LLP (the Company).
- 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 follows good practice;
- Protects the rights of clients, suppliers 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, where necessary, kept up to date;
5. Not be kept for longer than is necessary for that purpose or those purposes;
6. Be processed in accordance with the rights of data subjects under this Act;
7. Have appropriate technical and organisational measures taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data;
8. Not be transferred to a country or territory outside the European Economic Area
    1. unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.
    2. The Company complies with the conditions for transfer set out in Chapter V of the GDPR. https://gdpr-info.eu/chapter-5/ See article 49.

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 Partners are responsible for ensuring that the Company meets its legal obligations including:

- Keeping updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies periodically
- Handling data protection questions from anyone 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;
- 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 website policies/statements;

Guidelines

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

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to a Partner.
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 secure drawer or filing cabinet;
- 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.
- 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 Company;
- 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 except for essential business needs;
- 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, everyone 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 if appropriate.

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 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.
- 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;

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 to gdpr@toucaninternet.co.uk. The relevant data will be provided within 30 days.

The Company 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 and 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 Policy visit https://www.toucanweb.co.uk/legal