TOAD GDPR Policy

Introduction
TOAD hold personal data about employees, clients, suppliers and other individuals for a variety of business purposes. TOAD is committed to protecting the rights and freedoms of data subjects, by safely and securely processing their data in accordance with all of our legal obligations.

This policy describes how this personal data is collected, handled and stored to meet the company's data protection standards and to comply with the General Data Protection Regulation (GDPR).

This data protection policy ensures TOAD:

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

Data protection law
General Data Protection Regulation (GDPR) describes how organisations, including TOAD 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 state that personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- 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 TOAD
- All branches of TOAD
- All staff and volunteers of TOAD
- All contractors, suppliers and other people working on behalf of TOAD

It applies to all data that the company holds relating to identifiable individuals.
This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Social Profile URL (as LinkedIn cv)

Data protection risks

This policy helps to protect TOAD from 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 TOAD 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.

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.
- **TOAD 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 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 IT manager 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 also 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 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 or smartphones.
- 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 TOAD 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, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorised 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 TOAD 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 TOAD 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.
- TOAD will make it **easy for data subjects to update the information TOAD** holds about them. For instance, via the company website.
- 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 marketing manager'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 TOAD 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 an individual contacts the company 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 hello@toadlondon.com. The data controller can supply a standard request form, although individuals do not have to use this. The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Choosing how we use your data
We understand that you trust us with your personal information, and we are committed to ensuring you can manage the privacy and security of your personal information yourself.
With respect to the information relating to you that ends up in our possession, and recognising that it is your choice to provide us with your personally identifiable information, we commit to giving you the ability to do all of the following:

If you send us your personal data (such as through an email), you are agreeing to this policy and TOAD can store the data you send. You can at any time change, remove or request a copy of that data.

- You can verify the details you have submitted to TOAD by contacting us at hello@toadlondon.com. Our security procedures mean that we may request proof of identity before we reveal information, including your e-mail address and possibly your address.

- You can also contact us by the same method to change, correct, or delete your personal information controlled by TOAD at any time.

- You can always feel free to update us on your details at any point by contacting us.

- You can unsubscribe from receiving campaign emails from us by replying to this email with “unsubscribe”. Once you do this, you will no longer receive any emails from us.

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, TOAD will disclose the requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company’s legal advisers where necessary.

Providing information
TOAD 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 company has a privacy statement, setting out how data relating to individuals is used by the company.