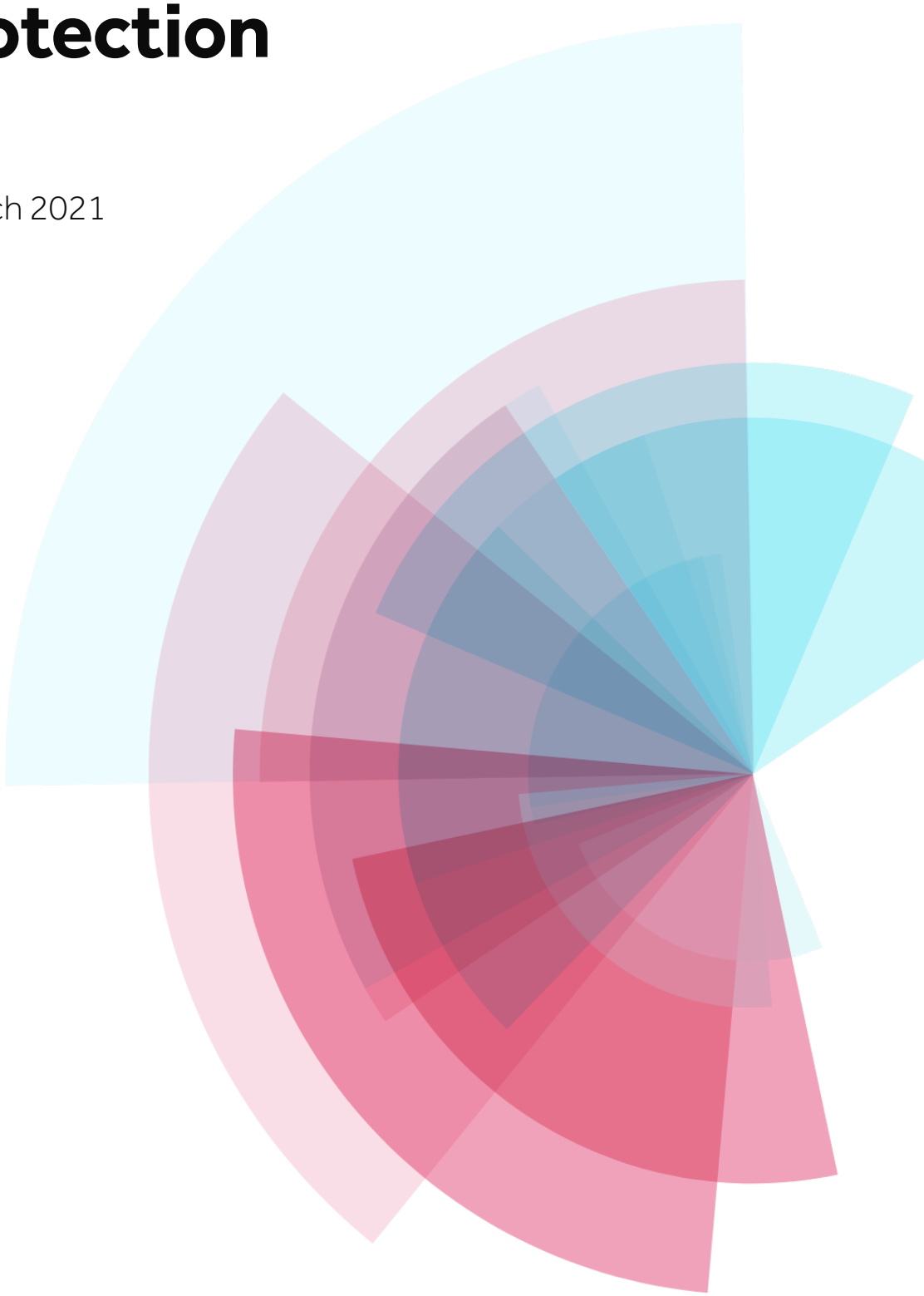
TGSN

Data Protection Policy

Last Updated March 2021



Contents

Introduction

TGSN needs to gather and store certain information about individuals. These can include clients, suppliers, business contacts, employees, projects beneficiaries, projects vendors, and other people the organization 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.

1. Context & Overview

1.1 Why this policy exists

This data protection policy ensures that TGSN:

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

1.2 Data Protection Law

The Data Protection Act 1998 describes how organizations – including TGSN – 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 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.

1.3 GDPR compliance

TGSN was keen on achieving GDPR compliance since the early founding of the company. For that, TGSN worked on implementing the guidelines and instructions of GDPR by:

- Establishing the lawful basis for the processing of data in its systems.
- Implementing practices to ensure the security of the data that the company processes.
- Implementing measures to establish accountability and governance over its data processing activities.
- Ensuring that the privacy rights of data owners are preserved and addressed.

The practices that TGSN implements to achieve GDPR compliance are clarified in this document.

2. Legal Foundation for Data Processing

TGSN uses the data that clients submit to its systems for the provision of its services. Additionally, TGSN uses the data for improving its services and products. More information about data uses can be found in the Data Use and Processing section of this document. Further, TGSN informs its clients about the way it uses their data upfront by signing a Data use agreement with the clients as well as agreeing with them on the company's data protection policy and privacy policy.

3. People, Risks & Responsibilities

3.1 Policy scope

This policy applies to:

- The head office of TGSN
- All branches of TGSN
- All staff and volunteers of TGSN
- All servers and databases managed by TGSN
- All contractors, suppliers and other people working on behalf of TGSN

It applies to all data that the company holds relating to identifi- able 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
- Any other information relating to individuals

3.2 Data protection risks

This policy helps to protect TGSN 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.

3.3 Responsibilities

Everyone who works for or with TGSN 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 TGSN meets its legal obligations.

The data protection officer 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 TGSN 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.

The IT manager 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 Marketing manager is responsible for:

- 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 principles.

4. Third Parties

TGSN utilizes the Microsoft Azure cloud services for the storage, processing and protection of all the data it stores on its systems. As per the Microsoft Azure SLA, it is ensured that all data stored is completely isolated and protected and that no third parties have access to that data. Other than that, TGSN shares none of the data it stores on its systems with any third party.

Occasionally, TGSN may run promotional campaigns, in which some statistical information may be mentioned about the client's projects and success stories. TGSN always obtains permissions prior to any use of data in such a way.

5. Privacy Rights

There are two classes of data that TGSN stores in its possession: *project data* and *client staff data*.

Project data is the data that the client submits to TGSN to assist in the use of TGSN systems; this data includes: information about projects, beneficiary information, vendor information, product information and invoice information.

Client staff data is the data that live on TGSN system that belong to the client staff that use the TGSN systems; client staff data include their names, phone numbers and emails.

TGSN ensures the protection and safe storage of both data classes and contractually guarantees the following rights to the client:

- The right to export all classes of data in a readable form and the right to receive their data.
- The right to correct any information the client stores on TGSN systems.
- The right to object to any of the ways TGSN processes client data.
- The right to destroy client data and remove it from TGSN systems.
- The right to know what third parties process client data and how.

The rights mentioned here are either offered as features built into TGSN systems or by means of formal requests that the client may submit to exercise any of their privacy rights.

6. Anonymous Information

TGSN collects anonymous information about the use and utilization of its systems for optimization and performance improvement purposes. This information does not reveal the identity of any of the users that use the system, nor does it contain any details that may jeopardize the identity of any stakeholders related to the system.

7. 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.
- TGSN 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 unauthorized 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.

8. System Security

Among the key principles and factors in the design of all TGSN systems is security. All TGSN systems implement measures that ensure highest levels of data and information protection and safety. The measures implemented include:

- Encryption of all data stored on all the components of the system.
- Secure network communication among the system components (the online portal, the terminal device).
- Data validation and verification of user input.
- Access control and user identification.
- Implementation of security measures against popular attacks such as DDoS.
- Automated and manual tests are run to ensure the system is immune against security attacks and vulnerabilities. These tests are regularly being experimented with, updated and improved and the implementation of security best practices is an ongoing operation in the company.

Further, the data that is stored and processed by TGSN systems is handled and protected to ensure its safety. Among the measures taken to protect data are:

- Sensitive data is encrypted with an encryption key that remains in the possession of the client. Meaning, that only the client can have access to that data.
- Access to data is restricted and controlled with mechanisms (see Data access control).

9. Data Handling

9.1 Data Storage and Protection

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 unauthorized 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 unauthorized 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 unauthorized 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 flash disks 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 approved cloud computing services.

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.

9.2 Data Use and Processing

In addition to using data to offer the services directly provisioned to the client, TGSN may use the data stored in its possession for three reasons: analyse the data to improve and optimize the system performance, introduce updates and bug fixes, and release new features and functionalities. The data used for these purposes is usually not the data that the data owner chooses to encrypt and conceal. However, in the event that encrypted data is needed for the mentioned reasons, TGSN informs the data owner about that.

Prior to processing client data, TGSN performed a *data protection impact assessment* that addressed the following:

- The need for the DPIA was identified.
- The nature of data processing was described.
- The people and entities that needed to be consulted about the data processing and the protection of data being processed were identified and consulted.
- The necessity for the processing of the data was assessed.
- Risks were identified and assessed and measures to reduce them were proposed and adopted.

9.3 Data Protection Awareness

When a TGSN worker, team or any other entity is awarded access to data, they're made aware of the importance of protecting the data in their possession. Further, data processors are provided with instructions on how to maintain the integrity of the data as well as protecting it against potential breaches.

Among the instructions given to data processors are:

- 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 authorized 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.

9.4 Data Accuracy

The law requires TGSN 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 TGSN 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.
- TGSN will make it easy for data subjects to update the information that TGSN 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.

9.5 Data Access Control

Access to data storage sources is restricted to a predefined list of people in the company, with predefined permissions and predefined activities that they can do with the data. These

people are in charge of disclosing specific portions of data upon the formal approval of the *data protection officer*. This ensures that unauthorized people cannot reach data storage sources, preventing potential breaches.

Records of data access are maintained internally and are controlled and updated by the data protection officer.

9.6 Data Disclosure

When a data set is to be accessed by any person, the person needs to make a formal request to the *data protection officer*. In the formal request, the person needs to list the reasons and motivations for accessing the data as well as how the data will be used. The officer reviews the request details, and then

based on the contractual commitments of TGSN with the data owner, the officer approves the disclosure of the requested data set to the person requesting the access.

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, TGSN will disclose 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.

9.7 Data Breaches

TGSN implements a procedure that regularly scans for potential data breaches and explores ways of preventing those from happening. In the event of a data breach that has a risk on data owners, the company is committed to announcing that breach and communicating it with:

- The relevant authorities in the UK through its office there.
- The authorities in Turkey.
- The people that are affected by the breach (including the client and the people whose personal data is stored on TGSN systems).

When data breaches occur, the company follows an internal procedure to investigate the reasons that caused the breach and implement measures to prevent similar breaches in the future.

10. Representation & Information Provision

TGSN 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.

Additionally, the company's office in the UK is responsible for addressing data protection-related matters.