TELCOM EST. 1999
Next Generation Voice and Data

DATA PROTECTION POLICY

May 2018

1. Contents

2. PURPOSE

This policy establishes an effective, accountable and transparent framework under which Telcom Limited ensures compliance with the EU Directive on GDPR.

3. POLICY STATEMENT

- **Our Commitment:** We are committed to conducting our business in accordance with all applicable data protection laws and regulations and in line with the highest standards of ethical conduct.
    - This policy sets forth the expected behaviour of our employees and third parties to secure the personal data of data subjects that is transferred by Data Controllers to our system.

4. DEFINITIONS AND SCOPE

a) SCOPE

- This policy applies to all parties responsible for the processing of personal data, whether employed or contracted, on behalf of Telcom Limited, henceforth collectively referred to in this document as 'the Company'.
- The Company is defined as a Data Processor only. Its customers are Data Controllers only. The Company does not have data subjects as its customers.

b) PERSONAL DATA

- Personal data is defined as the data that identifies or can be used to contact a person (e.g name, e-mail address, date of birth, user id); identifies a unique device used by a single person (e.g. an IP address or unique device IP); or reflects or represents a personal behaviour or activity (e.g. location, applications downloaded, websites visited).

c) DATA CONTROLLER

- A Data Controller is defined as the company or organisation that makes all the decisions about initially accepting data from the data subject (EU resident). The Data Controller must tell the supervisory authority the nature and scale of a breach and the actions taken to mitigate a breach.

d) DATA PROCESSOR

- A Data Processor is defined as the company or organisation that processes or stores data for the Data Controller.
- As a Data Processor, the Company provides Software as a Service (SaaS) to enable Data Controllers to:
    - Secure personal data of their data subjects at the application, network, cloud, or endpoint level.
    - We provide automated security threat intelligence, identify possible threats and advise on preventative actions to be taken to minimise the risk of a data breach.
    - We deploy data leak prevention (either by hacking or accidental leakage) solutions and in the event where a data breach is detected, we notify the Data Controller of what personal data has been compromised, what is the scale of the breach and we advise on what actions are necessary to eliminate the source of the leakage.
    - We apply policies to inspect and control content traversing the network to help limit unauthorised transfer of sensitive data.

5. Governance

a) Data Protection Officer

- To demonstrate our commitment to data protection, and to enhance the effectiveness of our compliance efforts, we have appointed a Data Protection Officer (Liam Tully).
- The Data Protection Officer operates with independence and is supported by suitability skilled individuals granted all necessary authority. In this capacity the Data Protection Officer reports to our M.D.
- Contact Details: liamtully@telcom.ie
- The Data Protection Officer's duties include:
    - Inform and advise us and our employees and contractors who carry out processing, on data protection regulations; on national law or European Union based data protection provisions.
    - Creates and maintains all relevant data protection procedures in support of this policy.
    - Acts as the point of contact for and cooperating with Data Protection Authorities and client Data Controllers.
    - Audits compliance by the company with this policy and related procedures.
    - Reports to the CEO and senior executives of the company on audit results, any data leakage occurrences and any corrective actions that arise.
    - Acts as the point of contact for Data Controllers in the event of a data leakage occurrence.
    - Keep all relevant records in support of the company's GDPR policy and procedures.

b) Compliance Monitoring

- To confirm that an adequate level of compliance is being achieved by us in relation to this policy, the Data Protection Officer will carry out an annual data protection compliance audit for the company. Each audit will, as a minimum, assess:
  - 100% compliance in the provision of our services to our data controllers.
  - Has there been any data breach notifications?
  - Review the adequacy of reporting and corrective actions in the event of all data breaches for each data controller and make recommendations for review by the CEO and the executive team.
  - Training records for employees on GDPR
- The Data Protection Officer, in cooperation with key business stakeholders, will devise a plan with a schedule for correcting any identified deficiencies within a defined and reasonable time frame. Any deficiencies or deviation from best practice will be reported to the executive team.

6. Data Protection Principles

We have adopted the following principles to govern the processing of personal data:

- Lawfulness, Fairness and Transparency: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- Purpose Limitation: Personal data shall be collected from data controllers for the purpose of protecting the data client's information from security threats.
- Data Minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accuracy: Personal data shall be accurate and, kept up to date.
- Storage Limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.
- Integrity & Confidentiality: Personal data shall be 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.
- Accountability: The Data Controller shall be responsible for and be able to demonstrate security compliance. The company will provide reporting and notifications to the data controller.

7. Data collection

a) Data Sources

Personal data will only be collected directly from the **Data Controllers**

b) Data subject Notification

- It is the responsibility of the Data Controller to provide data subject notifications in compliance with the requirements of GDPR.
- It is the responsibility of the Company to provide Data Breach Notifications to the Data Controller in the event of a data breach. The notification must identify the data subject(s) affected and the scale of the breach.
- These disclosures may be given orally (for urgency) and followed up electronically or in writing.

8. Data Use

a) Data processing (ONLY)

As a general guideline, we use personal data for the following broad purposes:

- **Gain complete visibility**. Our platform offers visibility into all traffic across the network, endpoint and cloud. It is classified by User ID, Application ID, and Content.
- **Reduce the attack surface.** The attack surface is expanding rapidly as companies' use of applications and devices proliferates. We reduce the attack surface by enabling only the allowed applications for the right user and deny everything else.
- **Prevent known threats.** Traffic that is allowed on the network is monitored, analysed and blocked where appropriate for exploits, malware, malicious URLs, and dangerous or restricted files or content. System administrators apply policies to inspect and control this content to eliminate unauthorised transfer of sensitive data.
- **Combine threat intelligence.** Customer data at the endpoint feeds into our global community of customers and provides us with the threat intelligence to block known malware and exploits before they can compromise the endpoint.
- **Mitigate unknown threats.** Our platform goes beyond stopping known threats to proactively identify and block unknown malware and exploits which are often used in sophisticated and targeted attacks. When a novel malware or exploit is seen our threat analysis service automatically creates and shares a new control to block the core techniques used by zero-day exploits and identify and block unknown malware from compromising endpoints.
- **Generate an alert.** If a policy is violated or a known or unknown threat is detected an alert is generated and automatic action taken to eliminate the risk.
- **Prevent accidental data leakage.**

b) Data Retention

To ensure fair processing, personal data will not be retained by us for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

9. Law Enforcement Requests & Disclosures

In certain circumstances, it is permitted that personal data be shared without the knowledge or consent of a data subject. This is the case where the disclosure of the personal data is necessary for any of the following purposes:

- The prevention or detection of crime.
- The apprehension or prosecution of offenders.
- By the order of a court or by any rule of law.

If any employee receives a request from a court or any regulatory or law enforcement authority for information relating to a data subject, they must immediately notify the Data Protection Officer who will provide comprehensive guidance.

a) Data Protection Training

- All employees who have access to personal data will have their responsibilities under this policy outlined to them as part of their staff induction training.
- In addition, we will provide regular Data Protection training and procedural guidance for our staff.

b) Data Transfers

- We may transfer personal data to internal or third-party recipients located in another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects.
- We may only transfer personal data where one of the transfer scenarios list below applies:
    - The transfer is necessary for the performance of a contract between the Data Controller and the data subject
    - The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the Data Controller or data subject.
    - The transfer is legally required on important public interest grounds.
    - The transfer is necessary for the establishment, exercise or defence of legal claims.
    -

c) Complaints handling

- Complaints in relation to the processing of personal data must be put forward in writing by the Data Controller to the designated Data Protection Officer.
- An investigation of the complaint will be carried out to the extent that is appropriate based on the merits of the specific case.
- The Data Protection Officer will inform the Data Controller of the progress and the outcome of the complaint.

d) Breach Reporting

- Any data breach that is detected will be automatically notified to the Data Controller. The notification will identify the nature of the breach and the scale of the breach.
- If a personal data breach is confirmed, the Data Protection Officer will follow the relevant authorised procedure based on the criticality and quantity of the personal data involved.
- For severe personal data breaches, our Executive Team will initiate and chair an emergency response team to coordinate and manage the personal data breach response.

e) Support, Advice and Communication

For advice and support in relation to this policy, please contact the Data Protection Officer by e-mail: liamtully@telcom.ie