Commsmultilingual

Saving you time, effort and reputation

GDPR POLICY

Prepared by: Operations Director

Approved by: CEO

Last Updated: 14th May 2018

Comms Multilingual Ltd.
Page House,
40 East Street,
Epsom,
Surrey,
KT17 1BB,
United Kingdom

Telephone: +1-888-361-5478 (USA & Canada, toll-free)
Telephone: +44 (0)1372 209 936 (UK & International)

Fax: +44 (0)1372 744382

Table of Contents

Key details

Organisation	Comms Multilingual Ltd. (CML)
Policy Operational Date	25th May 2018
Date Policy Approved by Management	14th May 2018
Policy Review Date	14th May 2019

Introduction

Comms Multilingual Ltd (CML) needs to gather and use certain information about individuals. These can include customers and potential customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet CML's data protection standards and to comply with the law.

The CML privacy policies provide detail on why personal data is being processed and what type of data and how individuals can exercise their rights in relation to that data. They also detail the legal basis under which the data is held.

Purpose of this Policy

This data protection policy ensures Comms:

- Complies with data protection law and follows good practice
- Protects the rights of clients, employees and providers
- Is open about how it stores and processes personal data
- Protects itself from the risks of a data breach

Policy Scope

This policy applies to:

- The head office of Comms Multilingual Ltd.
- All home offices of Comms Multilingual Ltd.
- All staff, interns and volunteers of Comms Multilingual Ltd.
- All contractors, providers and other people working on behalf of Comms Multilingual Ltd.

It applies to all data that the company holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:

- Names of individuals
- Postal addresses
- Email addresses

- Telephone numbers
- ID documents
- Any other information that would identify an individual

GDPR (General Data Protection Regulation)

The General Data Protection Regulation describes how organisations, such as CML, 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.

Personal data must:

- Be used lawfully, fairly and in a transparent manner in relation to individuals
- Be collected for specified, explicit and legitimate purposes
- Be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Be accurate and, where necessary, be kept up to date
- Be kept in a form that permits identification of data subjects for no longer than is necessary
- Be processed in a manner that ensures appropriate security of the personal data
- Be processed in accordance with the rights of data subjects
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Personal Data

"Personal data" is defined as any information relating to a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Data Controller

CML is a data controller and shall implement appropriate technical and organisational measures to ensure that the rights of individuals are protected by:

- Encrypting personal data.
- Ensuring the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.
- Restoring the availability and access to data in a timely manner in the event of a physical or technical incident.
- Regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Breach & Notification

In the event of a personal data breach, the CML data protection administrator will notify the appropriate supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it. CML will make every effort to ensure that any personal data breach is remedied as soon as possible.

However, CML will not notify the appropriate supervisory authority where the personal data breach is unlikely to result in a risk to the rights and freedoms of individuals.

Rights for Individuals

CML recognises the rights of individuals as follows:

- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right of data portability
- The right to object.
- Rights of automated decision making and profiling

Data Protection Risks

This policy helps to protect Comms Multilingual Ltd. from some data security risks, including:

- **Breaches of confidentiality** (e.g., information being given out inappropriately)
- **Failing to offer choice** (e.g., all individuals should be free to choose how the company uses data relating to them)
- **Reputational damage** (e.g., the company could suffer if hackers successfully gained access to sensitive data)
- **Harm to individuals** where data held is inaccurate or insufficient

Responsibilities

Everyone who works for or with CML has 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.

The following people have key areas of responsibility:

- The board of directors is ultimately responsible for ensuring that CML meets its legal obligations and for approving any unusual requests for disclosure of personal data.

- The Data Protection Administrator 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 and monitoring compliance.
    - Arranging data protection training and advice for the people covered by this policy.
    - Informing and advising employees of their obligations to comply with the GDPR and other data protection laws.
    - Handling data protection questions from employees and anyone else covered by this policy.
    - Dealing with requests from individuals to see the data that CML holds about them (also called 'subject access requests').
    - Checking and approving any contracts or agreements with third parties that may handle CML's sensitive data.
    - Ensuring that staff and subcontractors carry out regular IT equipment checks and scans to ensure security hardware and software is functioning properly.
    - Notifying breaches to the ICO.

- The IT managers are 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 outside organisations.
    - Where necessary, working with other staff to ensure marketing initiatives abide by 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 and provide the reasons why it is required.
- CML 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, according to the Comms data retention policy.
- Employees should request help from their manager or the data protection administrator if they are unsure about any aspect of data protection.

Data Storage

The following rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT managers 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 been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Staff and contractors and other people with access to personal data should make sure paper and printouts are not left where unauthorised people could see them (e.g., on a printer).
- Data printouts should be shredded and disposed of securely when no longer required.
- Where data is obtained via the telephone, it should be checked back with the individual to ensure accuracy.

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 or USB stick, 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 smart phones or USB devices.
- All servers and computers containing data should be protected by approved security software and a firewall.
- All personal data stored electronically should be **reviewed annually** and should be discarded according to the CML retention policy.

Data Use

- When working with personal data, employees and subcontractors should ensure the screens of their computers are always locked when left unattended.

- Personal data should not be shared informally.
- Data must be encrypted before being transferred electronically. The IT managers have the responsibility of explaining 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. The central copy of any such data must be accessed and updated as necessary.

Data Accuracy

The law requires Comms Multilingual Ltd. 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 confirming a customer's details when they call or regularly contacting providers to encourage them to inform CML of any changes to their data.
- CML. will make it easy for data subjects to update the information it holds about them. Currently, data subjects can request this by contacting CML. In the future, this will be done through our Project Management system, Plunet.
- Data should be updated as inaccuracies are discovered.
- It is the Sales Manager's responsibility to ensure that internal marketing databases are checked and updated annually.

Subject Access Requests

All individuals who are the subject of personal data held by Comms Multilingual Ltd. 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 administrator at data.protection@commsmultilingual.com.

The Data Protection Administrator will always verify the identity of anyone making a subject access request before handing over any information. An initial response to a Subject Access Request, containing all the requested data, must be provided within thirty days.

The supply of information under a Subject Access Request is generally free of charge. However, CML reserves the right to charge a reasonable fee when a request is manifestly unfounded or excessive, particularly where it is a repeat request.

Disclosing Data for Other Reasons

In certain circumstances, personal data may need to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CML will disclose requested data. However, the data protection administrator will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers, where necessary.

Providing Information

Comms Multilingual Ltd. 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. This statement is available on CML's website and a copy is also available on request from the data protection administrator.