DEPENDABLE ◆ FLEXIBLE ◆ DEFENSIBLE

TRANSLATION SERVICES

GDPR Policy

PREPARED BY: Sonia Sala, Operations Director

APPROVED BY: Sue Orchard, Director

LAST UPDATED: 23rd March 2022

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

Policy Information 3

GDPR (General Data Protection Regulation) 3

Introduction 3

Purpose of this Policy 4

Policy Scope 4

Definitions 5

Personal Data 5

Data Subjects, Data Controllers and Data Processors 5

Controllers and Processors 5

Privacy Management 7

Consent 7

Information Provided at Data Collection 8

Profiling 9

Rights for Individuals 10

Data Protection Risks 11

Responsibilities 11

General Staff Guidelines 12

General Client Guidelines 12

General Subcontractor Guidelines 13

Data Storage 13

Data Use 14

Data Accuracy 14

Subject Access Requests 14

Disclosing Data for Other Reasons 15

Providing Information & Transparency 15

Policy Information

Organisation	Comms Multilingual Ltd.
Policy Operational Date	14th May 2018
Date Policy Approved by Management	14th May 2018
Policy Review Date	23rd March 2022

GDPR (General Data Protection Regulation)

The **General Data Protection Regulation (GDPR)** (which came into force on 25th May 2018) is an European Union regulation on data protection. It provides a single set of rules on the use of "personal data". The objectives are to improve trust in the digital economy and to standardise European laws by offering a more consistent legal framework for data protection.

On 28 June 2021 the EU Commission adopted decisions on the UK's adequacy under the EU's General Data Protection Regulation (EU GDPR) and Law Enforcement Directive (LED). In both cases, the European Commission has found the UK to be adequate. This means that most data can continue to flow from the EU and the EEA without the need for additional safeguards after Brexit.

The GDPR is retained in domestic law as the UK GDPR, but the UK has the independence to keep the framework under review. The 'UK GDPR' sits alongside an amended version of the DPA 2018.

The key principles, rights and obligations remain the same for both regulations. However, there are implications for the rules on transfers of personal data between the UK and the EEA.

Both EU GDPR and UK GDPR apply to Comms Multilingual Ltd., as we are a UK-based business and we process personal data from the UK, EU and EEA. Any data processing and transfers are therefore supervised by the ICO and competent authorities in the EU or EEA.

Although CML needs to comply with EU GDPR, CML does not have any branch, office or establishment in the EU and our data processing is only occasional and low risk to the data protection rights of individuals, so we do not require a GDPR representative in the EEA.

EU GDPR and **UK GDPR** will be referred to as **GDPR**, and **Comms Multilingual Ltd**. will be referred to as **CML** for the purposes of this document.

Introduction

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 and GDPR 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

The goal of this policy is to depict the legal data protection aspects in one summarising document. It can also be used as the basis for statutory data protection inspections (e.g., by the customer within the scope of commissioned processing). This is not only to ensure compliance with the European and UK General Data Protection Regulation (GDPR) and Data protection Act (DPA) 2018, but also to provide proof of compliance.

This data protection policy ensures CML:

- 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 CML
- All home offices of CML
- All staff, interns and volunteers of CML
- All subcontractors, providers and other people working on behalf of CML

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

Personal data belongs to:

- Clients
- Employees
- Providers and subcontractors

Personal data may be found in:

- CML documentation, databases, Plunet and other administrative software
- Emails

- Documents for translation, Translation Memories and reference materials

Definitions

Personal Data

"Personal data" is defined in both the Directive and the GDPR as any information relating to an 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. There is no distinction between personal data about individuals in their private, public or work roles.

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

CML processes and stores personal data from clients, employees, providers and subcontractors. Processing of any personal data is only done for lawful and business purposes and CML has processes in place to ensure data minimisation and appropriate retention periods.

CML also reviews and updates personal data regularly to ensure data accuracy.

Personal data is only transferred outside the EEA for legitimate interest and CML obtains permission from data subjects and/or controllers before doing so.

Data Subjects, Data Controllers and Data Processors

GDPR distinguishes between "data subjects" (individuals), "data controllers" (organisations that determine the purpose and use of the personal data) and "data processors" (often third-party companies that process data on behalf of the data controller).

Controllers and Processors

GDPR separates responsibilities and duties of data controllers and processors, obligating controllers to engage only those processors that provide "sufficient guarantees to implement appropriate technical and organisational measures" to meet the Regulation's requirements and protect data subjects' rights.

Controllers and processors are required to "implement appropriate technical and organisational measures" taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals."

The regulation provides specific suggestions for what kinds of security actions might be considered "appropriate to the risk", including:

- The pseudonymisation and/or encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of systems and services processing personal data.
- The ability to restore the availability and access to data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Controllers and processors that adhere to either an approved code of conduct or an approved certification may use these tools to demonstrate compliance.

The controller - processor relationships must be documented and managed with contracts that mandate privacy obligations – ultimately controllers must assure themselves of processors privacy capabilities.

CML acts both as Data Processor and Controller:

- CML is the controller of personal data provided by clients, employees, providers and subcontractors.
- CML is only the controller of personal data in documents for translation, when such data is not used for the purposes for which the client provided the data.
- As data controller, CML will process personal data for legitimate interest and administrative purposes only. CML will also adhere to our Privacy Policy at all times when handling personal data.
- Personal data in translation files may be anonymised or encrypted when used for any purpose other than the translation of the documents. Alternatively, CML will request permission from the data subject or ensure that data is processed for legitimate interests only.
- CML is a data processor for data contained in translation files. In such cases, CML needs to ensure that the data controller has obtained permission from the data subject or is sending the data to CML for a legitimate interest.

Data Protection Officers

Data Protection Officers must be appointed for all public authorities, and where the core activities of the controller or the processor involve “regular and systematic monitoring of data subjects on a large scale” or where the entity conducts large-scale processing of “special categories of personal data” (such as that revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and the like). This is likely to apply to some of the larger scale Marketing Service Providers and Research Organisations – but needs further clarification.

Although an early draft of the GDPR limited mandatory data protection officer appointment to organisations with more than 250 employees, the final version has no such restriction.

The regulation requires that they have “expert knowledge of data protection law and practices.” The level of which “should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor.”

The data protection officer’s tasks are also delineated in the regulation to include:

- Informing and advising the controller or processor and its employees of their obligations to comply with the GDPR and other data protection laws.
- Monitoring compliance including managing internal data protection activities, training data processing staff, and conducting internal audits.

- Advising with regard to data protection impact assessments when required under Article 33.
- Working and cooperating with the controller's or processor's designated supervisory authority and serving as the contact point for the supervisory authority on issues relating to the processing of personal data.
- Being available for inquiries from data subjects on issues relating to data protection practices, withdrawal of consent, the right to be forgotten and related rights.

Data Protection Officers may insist upon company resources to fulfil their job functions and for their own ongoing training.

They must have access to the company's data processing personnel and operations, significant independence in the performance of their roles, and a direct reporting line "to the highest management level" of the company.

Data Protection Officers are expressly granted significant independence in their job functions and may perform other tasks and duties provided they do not create conflicts of interest.

The regulation expressly prevents dismissal or penalty of the data protection officer for performance of her tasks and places no limitation on the length of this tenure.

A company with multiple subsidiaries (a "group of undertakings") may appoint a single data protection officer so long as they are "easily accessible from each establishment."

The GDPR also allows the data protection officer functions to be performed by either an employee of the controller or processor or by a third-party service provider.

CML has determined that a Data Protection Officer is not required due to the nature of our activities.

However, CML has appointed a Data Protection Administrator, who acts as the main point of contact for any data protection related queries or incidents, and who will respond to any subject Access requests.

Privacy Management

The regulation mandates a "Risk Based Approach" where appropriate organisation's controls must be developed according to the degree of risk associated with the processing activities.

Where appropriate, privacy impact assessments must be made – with the focus on protecting data subject rights.

Data protection safeguards must be designed into products and services from the earliest stage of development – Privacy by Design.

Privacy-friendly techniques such as pseudonymisation are encouraged to reap the benefits of big data innovation while protecting privacy.

There is an increased emphasis on record keeping for controllers – all designed to help demonstrate and meet compliance with the regulation and improve the capabilities of organisations to manage privacy and data effectively. There is an exclusion for small businesses (less than 250 staff) where data processing is not a significant risk.

CML has put many processes and measures in place to ensure confidentiality and data security. This includes an initial risk assessment, a Data Security Management policy and appropriate technical resources.

Consent

Consent is a basis for legal processing (along with legitimate interests, necessary execution of a contract and others).

According to GDPR, consent means "any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed".

The purpose for which the consent is gained does need to be "collected for specified, explicit and legitimate purposes**".** In other words, it needs to be obvious to the data subject what their data is going to be used for at the point of data collection.

Consent should be demonstrable – in other words, organisations need to be able to show clearly how consent was gained and when.

Consent must be freely given – a controller cannot insist on data that's not required for the performance of a contract as a pre-requisite for that contract.

Withdrawing consent should always be possible – and should be as easy as giving it.

CML only process personal data for legitimate interest purposes and data is provided by data subjects and controllers for such purposes. Therefore explicit consent is not required.

Information Provided at Data Collection

The information that must be made available to a Data Subject when data is collected has been strongly defined and includes:

- the identity and the contact details of the controller and DPO;
- the purposes of the processing for which the personal data are intended;
- the legal basis of the processing;
- where applicable, the legitimate interests pursued by the controller or by a third party;
- where applicable, the recipients or categories of recipients of the personal data;
- where applicable, that the controller intends to transfer personal data internationally;
- the period for which the personal data will be stored, or if this is not possible, the criteria used to determine this period;
- the existence of the right to access, rectify or erase the personal data;
- the right to data portability;
- the right to withdraw consent at any time;
- and the right to lodge a complaint to a supervisory authority.

Importantly where the data has not been obtained directly from the data subject (perhaps using a 3rd party list) the list varies and includes:

- from which source the personal data originate;
- and the existence of any profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

- There are some exceptions – notably where the effort would be disproportionate and, importantly, where the information has already been provided to the data subject.

CML has appropriate data collection processes in place, as stated in our GDPR and Privacy Policy.

Profiling

The regulation defines profiling as any automated processing of personal data to determine certain criteria about a person. "In particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

Individuals have the right not to be subject to the results of automated decision making, including profiling, which produces legal effects on him/her or otherwise significantly affects them. So, individuals can opt out of profiling.

Automated decision making will be legal where individuals have explicitly consented to it, or if profiling is necessary under a contract between an organisation and an individual, or if profiling is authorised by EU or Member State Law.

CML does not do profiling.

Legitimate Interests & Direct Marketing

The regulation specifically recognises that the processing of data for "direct marketing purposes" can be considered as a legitimate interest.

Legitimate interest is one of the grounds, like consent, that an organisation can use in order to process data and satisfy the principle that data has been fairly and lawfully processed.

The act says that processing is lawful if "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

CML may contact potential clients and prospects for marketing purposes. Contact and personal data will have been obtained lawfully by CML, in most cases directly from the data subject, and any marketing campaigns will fall into the legitimate interest category.

Breach & Notification

According to the regulation, a "personal data breach" is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

It's important to note that the wilful destruction or alteration of data is as much a breach as theft.

In the event of a personal data breach, data controllers must notify the appropriate supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it." If notification is not made within 72 hours, the controller must provide a "reasoned justification" for the delay.

Notice is not required if "the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals".

Importantly, when a data processor experiences a personal data breach, it must notify the controller but otherwise has no other notification or reporting obligation.

Should the controller determine that the personal data breach "is likely to result in a high risk to the rights and freedoms of individuals", it must also communicate information regarding the personal data breach to the affected data subjects. Under Article 32, this must be done "without undue delay."

The GDPR provides exceptions to this additional requirement to notify data subjects in the following circumstances:

1. The controller has "implemented appropriate technical and organisational protection measures" that "render the data unintelligible to any person who is not authorised to access it, such as encryption."
2. The controller takes actions subsequent to the personal data breach to "ensure that the high risk for the rights and freedoms of data subjects" is unlikely to materialise.
3. When notification to each data subject would "involve disproportionate effort," in which case alternative communication measures may be used.

As stated in our GDPR and Privacy Policy, CML has a dedicated email and postal address to notify any suspected data breaches or incidents. Such notifications will be handled by the Data Protection Administrator according to set procedures that are compliant with GDPR requirements.

Rights for Individuals

GDPR strengthens the rights of UK and EU citizens and gives them greater control over what companies can do with their personal data. Under GDPR, data subjects typically have:

- **The right of access:** They have the right to know exactly what information is held about them and how it is processed.
- **The right of rectification:** They are entitled to have their personal data rectified if they think some of it is inaccurate or incomplete.
- **The right to erasure:** Also known as the right to be forgotten. This refers to an individual's right to have their personal data deleted.
- **The right to restrict processing:** They have the right to block or suppress the processing of their personal data.
- **The right to data portability**: This allows individuals to retain and reuse their personal data for their own purpose.
- **The right to object**: Individuals are entitled to object to their personal data being used for purposes, such as direct marketing or research.
- **Rights of automated decision making and profiling:** GDPR protects individuals against the risk that a potentially damaging decision is made without human intervention. For example, individuals can choose not to be the subject of a decision where the consequence has a legal bearing on them or is based on automated processing.

The data controller must demonstrate compliance with the fundamental data-processing principles. This is the principle of accountability. Other fundamental principles that need to be upheld are: lawfulness; fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; and integrity and confidentiality.

As stated in our GDPR and Privacy Policy, CML ensure that all data subjects have the rights above.

Data Protection Risks

This policy helps to protect CML 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)

CML has a Privacy Impact Assessment form that can help to assess risks and procedures in place in case of data breaches.

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 are those who need it for their work.
- Employees should always analyse documentation, files for translation, TMs and reference materials to check if they contain any personal data. If they do, they should discuss this with their manager.
- Personal data should be kept strictly confidential at all times and should not be shared with unauthorised people, either within the company or externally.
- When access to confidential information is required, employees can request it from their line managers and provide the reasons why it is required.
- CML provides training to help employees understand their responsibilities when handling personal data. This includes an initial training session during the onboarding process and an annual session with the rest of the staff.
- CML employees also sign data protection clauses in their contracts.
- Employees should request help from their manager or the data protection administrator if they are unsure about any aspect of data protection.
- Personal data must be encrypted before being transferred electronically. Employees should use Plunet to store and transfer files securely. Two-factor authentication (2FA) provides an extra level of protection.
- Employees should never send personal data outside of the European Economic Area. If this is required to complete a task, they should speak with their manager.
- Personal data should be regularly reviewed and updated if it is out of date. This includes updating customer or provider information in our systems and documentation, but also providing updated information to the relevant manager if the employee's details change.
- If personal data is no longer required, employees should delete it according to the CML data retention policies.

General Client Guidelines

- Clients should inform CML if their documentation contains personal data.
- CML may need to delete personal data from files, TMs and reference materials, or ensure that the client has legal basis for the processing of the data and gives their consent for CML to use it for the purposes of the job and in the countries where the data will be processed. If the client does not give their consent, CML should advise them of the implications.
- If the client agrees to the data processing, CML needs to enter into a **Data Processing Agreement (DPA)** with the client. As Controllers, clients should provide their own DPA, unless an agreement already exists. CML has its own DPA that can also be used.
- Clients also need to be informed of the use of any TMs with personal data and the use of TM software should be optional, and the subject of informed choice. Clients may prefer not to have their documents processed

through TM software due to data privacy issues. In this case CML should advise them of the potential disadvantages of their decision.

- File retention periods will be made known to the client upon request.

General Subcontractor Guidelines

- The only people able to access data covered by this policy are those who need it for their work.
- CML subcontractors sign data protection clauses in their contracts.
- CML subcontractors should keep all data secure, by taking sensible precautions and following the guidelines below. In particular, they should transfer and store data securely and strong passwords must be used and never be removed or shared.
- Personal data should not be disclosed to unauthorised people under any circumstances.
- Data should be deleted and disposed of as soon as work is completed or as dictated by law.
- CML subcontractors should request help from their CML contact 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 CML 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 or accessing available date in their Plunet profile.
- Data should be updated as inaccuracies are discovered.
- It is the Sales Manager's responsibility to ensure that internal marketing records are checked and updated annually.

Subject Access Requests

All individuals who are the subject of personal data held by CML 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 (SAR).

Subject access requests from individuals should be made by email, addressed to the data administrator at data.protection@commsmultilingual.com. All employees are trained to recognise a SAR should they receive it, and to know that they should discuss this with the data administrator.

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.

In accordance with GDPR, the deadline may be extended by up to two months, where requests are particularly "complex or numerous." If this is the case, the data subject must be contacted within one month of making their request and informed why an extension is necessary.

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.

CML keeps a written record of all SARs.

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 & Transparency

CML aims to ensure that individuals are aware that their data is being processed and that they understand:

- What data CML holds
- How the data is being used to ensure it is processed fairly
- 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;
- a training presentation for employees with information on GPDR. Training sessions are conducted with all new employees and annually with all staff;
- a guide for employees and a guide for providers including information on the data CML holds, how data is processed and their rights and obligations;
- information on GPDR embedded in agreements and handbooks for employees and providers;
- and subject access request forms available for employees and providers.

All information above is concise, transparent, intelligible and easily accessible.