Data Protection Policy

Introduction

In May of 2017 the GDPR laws came into effect and they fundamentally changed the way we treat personal data and the owners of the data.

This policy is in place to ensure all staff (including temporary and contractors), visitors and students are aware of their responsibilities and outlines how LMA complies with the core principles of GDPR in relation to LMA's approach to data protection and erasure.

LMA recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory and regulatory obligations, to ensure the protection of personal information and to enable the effective management of LMA. This policy and related documents meet the standards and expectations set out by contractual and legal requirements and has been developed to meet the best practices of business records management, with the aim of ensuring a structured approach to document control.

Effective and adequate records, and data management is necessary to:

- Ensure that LMA conducts itself in a structured, efficient and accountable manner
- Ensure that LMA realises best value through improvements in the quality and flow of information and greater coordination of records and storage systems
- Support core business functions and provide evidence of conduct and the appropriate maintenance of systems, tools, resources and processes
- Meet legislative, statutory and regulatory requirements
- Deliver services to, and protect the interests of, employees, clients and stakeholders in a consistent and equitable manner
- Assist in document policy formation and managerial decision making
- Provide continuity in the event of a disaster or security breach
- Protect personal information and data subject rights
- Avoid inaccurate or misleading data and minimise risks to personal information
- Erase data in accordance with the legislative and regulatory requirements Information held for longer than is necessary carries additional risk and cost and can breach data protection rules and principles.

LMA only ever retains records and information for legitimate or legal business reasons and always complies fully with the data protection laws, guidance and best practice.

Purpose

The purpose of this document is to provide LMA's statement of intent on how it provides a structured and compliant data and records management system. We define 'records' as all documents, regardless of the format; which facilitate activities, and are thereafter retained to provide evidence of transactions and functions.

Such records may be created, received or maintained in hard copy or in an electronic format with the overall definition of records management being a field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use, distribution, storage and disposal of records.

Scope

This policy applies to all staff within LMA (meaning permanent, fixed term, and temporary staff, any third-party representatives or subcontractors, agency workers, volunteers, interns and agents engaged with LMA in the UK or overseas). Adherence to this policy is mandatory and noncompliance could lead to disciplinary action.

Personal Information and Data Protection

LMA needs to collect personal information about the people we employ, work with or have a business relationship with, to effectively and compliantly carry out our everyday business functions and activities, and to provide the products and services defined by our business type. This information can include (but is not limited to), name, address, email address, data of birth, IP address, identification number, private and confidential information, sensitive information and bank details.

In addition, we may occasionally be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations. We are committed to collecting, processing, storing and destroying all information in accordance with the General Data Protection Regulation, UK data protection law and any other associated legal or regulatory body rules or codes of conduct that apply to our business and/or the information we process and store.

Our Data Protection Policy and processes comply fully with the GDPR's fifth Article 5 principle:

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 are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

Objectives

A record is information, regardless of media, created, received, and maintained which evidences the development of, and compliance with, regulatory requirements, business practices, legal policies, financial transactions, administrative activities, business decisions or agreed actions.

It is LMA's objective to implement the necessary records management procedures and systems which assess and manage the following processes:

- The creation and capture of records
- Compliance with legal, regulatory and contractual requirements
- The storage of records
- The protection of record integrity and authenticity
- The use of records and the information contained therein
- The security of records
- Access to and disposal of records

Records contain information that is a unique and invaluable resource to LMA and are an important operational asset. A systematic approach to the management of our records is essential to protect and preserve the information contained in them, as well as the individuals such information refers to. Records are also pivotal in the documentation and evidence of all business functions and activities.

LMA's objectives and principles in relation to Data Protection are to:

- Ensure that LMA conducts itself in an orderly, efficient and accountable manner
- Support core business functions and providing evidence of compliant protection, erasure and destruction
- To develop and maintain effective and adequate records management to ensure effective archiving, review and destruction of information
- To only retain personal information for as long as is necessary
- Comply with the relevant data protection regulations, legislation and any contractual obligations
- Ensure the safe and secure disposal of confidential data and information assets Ensure that records and documents are retained for the legal, contractual and regulatory period stated in accordance with each bodies rules or terms.
- Ensure that no document is retained for longer than is legally or contractually allowed

Guidelines and Procedures

LMA manage records efficiently and systematically, in a manner consistent with the GDPR requirements, and this policy is widely disseminated to ensure a standardised approach to data Protection and records management.

Records will be created, maintained and retained to provide information about, and evidence of LMA's transactions, customers, employment and activities. Protection schedules will govern the period that records will be retained and will be found in the published Schedule.

It is our intention to ensure that all records and the information contained therein is:

- Accurate - records are always reviewed to ensure that they are a full and accurate representation of the transactions, activities or practices that they document
- Accessible - records are always made available and accessible when required (with additional security permissions for select staff where applicable to the document content)
- Complete - records have the content, context and structure required to allow the reconstruction of the activities, practices and transactions that they document
- Compliant - records always comply with any record keeping legal and regulatory requirements
- Monitored – staff, LMA and system compliance with this Data Protection Policy is regularly monitored to ensure that the objectives and principles are being complied with at all times and that all legal and regulatory requirements are being adhered to.

Protection Period Protocols

All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All LMA and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

For all data and records obtained, used and stored within LMA, we:

- Carry out periodical reviews of the data retained, checking purpose, continued validity, accuracy and requirement to retain
- Establish periodical reviews of data retained
- Establish and verify protection periods for the data, with special consideration given in the below areas:
    - the requirements of LMA
    - the type of personal data
    - the purpose of processing
    - lawful basis for processing
    - the categories of data subjects

- Where it is not possible to define a statutory or legal protection period, as per the GDPR requirement, LMA will identify the criteria by which the period can be determined and provide this to the data subject on request and as part of our standard information disclosures and privacy notices
- Have processes in place to ensure that records pending audit, litigation or investigation are not destroyed or altered
- Transfer paper based records and data to an alternative media format in instances of long protection periods (with the lifespan of the media and the ability to migrate data where necessary always being considered)

Designated Owners

All systems and records have designated owners throughout their lifecycle to ensure accountability and a tiered approach to data protection and destruction. Owners are assigned based on role, area and level of access to the data required. Data and records are never reviewed, removed, accessed or destroyed with the prior authorisation and knowledge of the designated owners. These owners will

also be responsible for continually reviewing the protection schedule for items that they own, ensuring accuracy by updating the schedule accordingly if any protection periods or details have changed.

Suspension of Record Disposal for Litigation or Claims

If LMA is served with any legal request for records or information, any employee becomes the subject of an audit or investigation or we are notified of the commencement of any litigation against LMA, we will suspend the disposal of any scheduled records until we are able to determine the requirement for any such records as part of a legal requirement.

Storage & Access of Records and Data

Documents are grouped together by category and then in clear date order when stored and/or archived. Documents are always retained in a secure location, with authorised personnel being the only ones to have access. Once the protection period has elapsed, the documents are either reviewed, archived or confidentially destroyed depending on their purpose, classification and action type.

Expiration of Protection Period

Once a record or data has reached its designated protection period date, the designated owner should refer to the Protection register for the action to be taken. Not all data or records are expected to be deleted upon expiration; sometimes it is sufficient to anonymise the data in accordance with the GDPR requirements or to archive records for a further period.

Destruction and Disposal Of Records and Data

All information of a confidential or sensitive nature on paper, card, microfiche or electronic media must be securely destroyed when it is no longer required. This ensures compliance with the Data Protection laws and the duty of confidentiality we owe to our employees, clients and customers.

LMA is committed to the secure and safe disposal of any confidential waste and information assets in accordance with our contractual and legal obligations and that we do so in an ethical and compliant manner. We confirm that our approach and procedures comply with the laws and provisions made in the General Data Protection Regulation (GDPR) and that staff are trained and advised accordingly on the procedures and controls in place.

Paper Records

Due to the nature of our business, LMA retains paper based personal information and as such, has a duty to ensure that it is disposed of in a secure, confidential and compliant manner. LMA utilises onsite-shredding or a professional shredding service provider to dispose of all paper materials.

Electronic and IT Records and Systems

LMA uses a variety of systems, computers and technology equipment in the running of its business. From time to time, such assets must be disposed of and due to the information held on these whilst they are active; this disposal is handled in an ethical and secure manner.

The deletion of electronic records must be organised in conjunction with the IT Department who will ensure the removal of all data from the medium so that it cannot be reconstructed. When records or data files are identified for disposal, their details must be provided to the designated owner to maintain an effective and up to date register of destroyed records.

Only the Technical Support Department can authorise the disposal of any IT equipment and they must accept and authorise such assets from the department. Where possible, information is wiped from the equipment through the use of software and formatting, however this can still leave imprints or personal information that is accessible and so we also comply with the secure disposal of all assets.

Cookies

Our website may place and access certain first party Cookies on your computer or device. First party Cookies are those placed directly by LMA and are used only by LMA.

LMA use Cookies to facilitate and improve your experience of the LMA website and to provide and improve Our products and services. By using the LMA website users may also receive certain third party Cookies on their computer or device. Third party Cookies are those placed by websites, services, and/or parties. LMA use third party Cookies on the website. In addition, the LMA website uses analytics services provided by Google and Facebook, which also use Cookies. Website analytics refers to a set of tools used to collect and analyse usage statistics, to have a better understanding of the people using the website.

Erasure

In specific circumstances, data subjects have the right to request that their personal data is erased. However LMA recognise that this is not an absolute 'right to be forgotten'. Data subjects only have a right to have personal data erased and to prevent processing if one of the following conditions applies:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data must be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

Where one of the above conditions applies and LMA received a request to erase data, LMA first ensure that no other legal obligation or legitimate interest applies. If LMA are confident that the data subject has the right to have their data erased, this is carried out.

These measures enable LMA to comply with a data subject's right to erasure, whereby an individual

can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst standard procedures already remove data that is no longer necessary, LMA still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.
Where a request to erase and/or remove personal information from a data subject is received, the following process is followed:

1. The request is allocated to the Data Protection Officer
2. The DPO locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended
3. The request is reviewed to ensure it complies with one or more of the grounds for erasure:
    a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
    b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing
    c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing
    d. the personal data has been unlawfully processed
    e. the personal data must be erased for compliance with a legal obligation
    f. the personal data has been collected in relation to the offer of information society services to a child
4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received
5. The DPO writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure

If for any reason, LMA are unable to act in response to a request for erasure, LMA always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. **Such refusals to erase data include:**

- Exercising the right of freedom of expression and information
- Compliance with a legal obligation for the performance of a task carried out in the public interest
- For reasons of public interest in the area of public health
- For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing
- For the establishment, exercise or defence of legal claims

Special Category Data

In accordance with GDPR requirements and Schedule 1 Part 4 of The Data Protection Act 2018, organisations are required to have and maintain appropriate policy documents and safeguarding measures for the protection and erasure of special categories of personal data and criminal convictions etc. Our methods and measures for destroying and erasing data are noted in this policy and apply to all forms of records and personal data, as noted on our protection register schedule.

Compliance and Monitoring

LMA is committed to ensuring the continued compliance with this policy and any associated legislation and undertake regular audits and monitoring of our records, their management, archiving
and protection. Information asset owners are tasked with ensuring the continued compliance and review of records and data within their remit.

Responsibilities

Operational managers and information asset owners have overall responsibility for the management of records and data generated by their departments' activities, namely to ensure that the records created, received and controlled within the purview of their department, and the systems (electronic or otherwise) and procedures they adopt, are managed in a way which meets the aims of this policy.

Where a DPO has been designated, they must be involved in any data protection processes and records or all archiving and destruction must be retained. Individual employees must ensure that the records for which they are responsible are complete and accurate records of their activities, and that they are maintained and disposed of in accordance with LMA's protocols.

How long should records be kept for?

All projects are required to retain documents for a period after the activity has ended and these should be kept in an acceptable format so that they can be inspected where necessary. These are detailed in LMA's Data Protection Schedule.

Document Title	Data Protection Policy
Author	Kevin Sutherland, Principal
Date published	July 2021
Review planned	July 2022