LGMA
Local Government
Management Agency

Data Protection Policy

Approved: Executive 01.03.2021

Contents

Revision and Approval History					
Version	**Revised By**	**Revision Date**	**Approved By**	**Approval Date**	**Comments**
Ver 1.00	Yvonne McKeown	07.01.2021 (BH Consulting)			
Ver 1.2	Corporate Services	Rebranding	Executive	15/2/21	

1.Policy

This document sets out the policy for the Local Government Management Agency ("**LGMA**") regarding compliance with Irish data protection law.

The Local Government Management Agency "LGMA" complies with the General Data Protection Regulation ("**GDPR"**) and the Data Protection Acts 1988 to 2018 ("**Data Protection legislation**"). The LGMA is responsible for ensuring that only personal data that is actually needed is held, that it is held securely, for as long as it is needed, and for the specific purposes for which it was obtained.

The LGMA acts as a data controller for both employees, vendor and client data.

2. Definitions

GDPR: General Data Protection Regulation.

Consent: Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or, or access to, personal data transmitted, stored or otherwise processed.

Data Controller: A person who, either alone or with others, controls the contents and use of personal data.

Data Processor: An entity that processes personal data under the Data Controller's instructions.

Data Subject: An individual who is the subject of personal data.

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

Data Protection Impact Assessment (DPIA): A process designed to identify and address the privacy issues of a particular project. It considers the future consequences of a current or proposed action by identifying any potential privacy risks and then examining ways to mitigate or avoid those risks.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Recipient: A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Special Categories of Data: Special categories of data is defined in the Data Protection Acts as any personal data as to -

(a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject
(b) whether the data subject is a member of a trade union
(c) the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,
(d) the physical or mental health or condition or sexual life of the data subject

Responsibilities

All employees shall:

- Be aware of the LGMA's data protection requirements, and their roles and responsibilities in relation to their implementation.
- Maintain the personal data as confidential and secure at all times.
- Be bound by a duty of confidentiality.

3. Principles of GDPR

Principle 1 Obtain and Process Information Fairly

The GDPR requires that the LGMA must have a valid lawful basis for collecting and processing any of the personal data being processed.

Under GDPR there are six lawful bases for the processing of personal data which can be relied upon:

(a) Consent: The basis of consent requires a very clear and specific statement of consent for their personal data to be processed for specific purpose with a positive opt-in.

(b) Contract: The LGMA can rely on this lawful basis if they need to process personal data to fulfil contractual obligations or because they have requested specific steps are

taken before entering into a contract (e.g., contract of employment). The processing must be necessary to fulfil these obligations.

(c) Legal obligation: The LGMA can rely on this lawful basis when the processing is necessary to comply with a statutory obligation (not including contractual obligations).

(d) Vital interests: The LGMA can rely on this lawful basis where the data processing is required to protect someone's life.

(e) Public task: An organisation can rely on this lawful basis 'in the exercise of official authority' or to perform a specific task in the public interest that is set out in law.

(f) Legitimate interests: the processing is necessary for the legitimate interests of the LGMA or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. Note: The LGMA can only use legitimate interest in some circumstances as it cannot be used by public authorities in the performance of their duties.

The LGMA must determine the lawful basis, or reason, for collecting and processing the personal data before initiating the process.

1. The lawful basis for the collection and processing of the personal data must be provided to the Data Subject in advance of the data collection. This is available on the website at Privacy Statement - LGMA.
2. Where consent is used as the lawful basis, it must be freely given, specific, informed and unambiguous. When relying on consent, the LGMA shall:
    - Provide clear information on what the consent relates to.
    - Give the Data Subject sufficient information to make a choice.
    - Explain the different ways the LGMA shall use their information.
    - Provide a clear and simple way for the Data Subject to indicate they agree to different types of processing. The consent forms shall provide Data Subjects with the choice to consent to their information being used for one purpose but not another.
3. Consent may be withdrawn at any stage and separate consent must be obtained for different processing operations.
4. The LGMA shall have information materials and guidance that explains how the Data Subjects' personal information is used. This shall be provided in a format that can be easily understood. The LGMA shall provide employees with an Employee Privacy Notice that clarifies the purpose and uses of the employee's personal data.

Principle 2 Keep personal data only for one or more specified, explicit and lawful purposes

1. The LGMA must inform Data Subjects of the purpose of collecting and storing personal data and if consent is the legal basis appropriate consent must be provided prior to any data processing. The purposes of the processing must be precisely and fully identified prior to, or at the moment of the collection.
2. Personal Data can only be used for the purpose the LGMA has specified it was collected for.
3. Personal data collected for a specific purpose may be further processed for different purposes provided that these are not incompatible with the initial purposes. If the LGMA wishes to change or add an additional purpose which is not compatible with the original purpose, then the Data Subject must be made aware of the additional purpose for which the personal data will be processed.
4. Individuals have the right to request that the LGMA restricts the processing of their personal data in the following circumstances:
    - the individual contests the accuracy of their personal data and the LGMA is in the process of verifying the accuracy of the data.
    - the data has been unlawfully processed (i.e., in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead.
    - The LGMA no longer needs the personal data but the individual needs the LGMA to keep it in order to establish, exercise or defend a legal claim; or
    - An individual can make a request for restriction verbally or in writing and the LGMA has one calendar month to respond to a request.

Principle 3: Personal data shall be used and disclosed only in ways compatible with these purposes

As in Principle 2 above, the LGMA must inform Data Subjects precisely of the purpose of collecting and storing the personal data prior to, or at the moment of the collection.

Principle 4: Keep it safe and secure

Any changes to the LGMA processes, that may impact on the quality and safety of the service provided, shall be managed in accordance with Change Control. As part of this process, proposed changes shall be considered in relation to the potential impact on the safety and security of personal data. Where appropriate, through the use of Data Protection Impact Assessments (DPIA's), the LGMA shall embed data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This shall ensure that all required controls are implemented to protect Data Subject's personal information prior to the implementation of the change and therefore implementing data protection by design.

Principle 5: Keep it accurate, complete and up to date

The LGMA has an obligation to ensure that only accurate personal data is held on file. Personal data should be updated where necessary.

Principle 6: Ensure that it is adequate, relevant and not excessive

1. The LGMA must make sure the personal data is adequate and is processed/used fairly and effectively. The information sought should be:
    - Adequate in relation to the purpose(s) for which it was sought.
    - Relevant in relation to the purposes for which it was sought.
    - Not excessive in relation to the purposes for which it was sought.
2. The LGMA must not ask for, process or hold personal data that is not relevant or needed for the purpose(s) for which it was obtained.
3. Data deletion and destruction controls are implemented as detailed in the Retention Policy

Principle 7: Retain it for no longer than is necessary for the purpose or purposes

1. The LGMA ensures there is a clear policy for the retention and disposal of personal data they no longer require. The retention times for personal data shall be detailed within the Record of Processing.
2. Timeframes for retention of personal data should be clearly communicated to Data Subjects at the outset.

Principle 8: Give a copy of his/her personal data to an individual, on request

The LGMA must comply with a Subject Access Request under GDPR within 1 month.

4. Personal Data Protection and Security Measures

The LGMA shall implement effective data security measures for personal data. In deciding what level of security is appropriate, the LGMA shall have regard to the nature of the personal data in question, and the harm that might result from unauthorised use, disclosure or loss of the personal data.

Physical Securities for Hardcopy Personal Data

1. The designated location utilised to retain personal data records shall have secure windows, doors and a controlled access system. This location shall allow for controlled access and speedy retrieval of records when and where they are required by authorised individuals but also provide controls to prevent unauthorised access.

2. Personnel data shall be protected from hazards such as fire, flooding, temperature, humidity, atmospheric pollution and vandalism by use of a fireproof cabinet that can be locked when not in use. The keys of locked filing cabinets shall be stored in a secure location and employees are prohibited from taking such keys home.
3. All employees shall ensure that personal data is guarded securely at all times and shall take care to ensure that the Data Subjects information is not placed in any public place or where it may be viewed or accessed inappropriately.

- Personal data shall not be left on desks in offices in the absence of the responsible employee. Whenever an office is left unattended it should be securely locked.
- All personal data records shall be returned to their appropriate storage facility as soon as reasonably possible after use.
- Personal data in printed format shall not be left unattended at the reception desk or in the canteen/kitchen.

4. All waste papers, printouts, etc. of personal data shall be stored in secure lockable confidential waste bins that have a bin top or slot through which confidential waste can be placed but not retrieved. This applies to all areas of the LGMA, including office areas to which access is restricted to employees. Wastepaper shall be disposed of via confidential shredding by an approved supplier.
5. Where keypad access controls are in use for certain areas of the LGMA, the key codes shall be changed periodically.
6. Postal correspondence, such as incoming and outgoing letters, that is awaiting collection or further distribution within the LGMA, shall be held in a secure environment.

5. Software Securities for Data

Where the records of Data Subjects are retained via software systems, the LGMA shall use technical security measures to protect the data. Minimum standards of security implemented by the LGMA shall include the following:

1. Implementation of software controls to prevent external hacking and access by the cloud provider's personnel or by other users. Anti-virus software shall be used and shall be kept up to date.
2. Access to central IT servers shall be restricted in a secure location with only a limited number of employees having access. The access for these individuals to the central IT server are approved by the LGMA, including any non-authorised employees or contractors.
3. Secure backup systems shall be in place for vital personal data. There shall be a back-up procedure in operation for data held on computer. This shall include an off-site back up.

4. Personal data on computer screens should be hidden from the view of passers-by at all times. Computer screens shall be set to automatically lock and log users off after a certain short period of inactivity. A screen saver shall appear on locked screens to ensure that no personal data remains visible.
5. Individual passwords for systems shall be used to stop unauthorised access to records. PC's and laptops shall utilise encryption software. The standard of encryption shall be sufficiently robust to withstand attacks from newly developed decryption software.
6. Transmission of personal data over external networks, such as the internet, should normally be subject to robust encryption.
7. Access to personal data held in soft copy will be allocated in accordance with the roles and responsibilities of the employee.
8. Employees are prohibited from accessing or editing, via other users' accounts, the records of personal data on the LGMA's computer systems
9. Where IT management and securities are managed by an external supplier, the supplier shall be formally approved, and a Data Processing Agreement shall be in place covering the security of the data that meets or exceeds the assessed level of protection required.
10. The Data Subject's personal information shall not be discussed by employees outside the LGMA or in the LGMA corridors, lifts or canteen.

6. Data Processing Agreement

All data processing arrangements with third party service providers shall meet the requirements of the Data Protection Acts 1988 to 2018 and the requirements of the GDPR.

Where the LGMA engages the services of a Data Processor, it shall take certain steps to ensure that the data protection standards are maintained. A Data Processor shall be engaged to complete data processing for the LGMA under a written contract, which details appropriate data securities and safeguards.

Any contract utilised for the engagement of a Data Processor shall specify:

- The subject matter of the data and duration of the processing.
- The type of personal data and categories of data subject.
- The obligations and rights of the LGMA as the Data Controller.
- The instructions as to what the Data Processor can do with the personal data provided.
- The nature and purpose of the processing, that the Data Processor will process personal data only on the basis of the authorisation and instructions received from the Data Controller. This provision ensures that personal data

passed on to a Data Processor may not be retained or used by the data processor for its own purposes.

- That the Data Processor must be committed to apply appropriate security measures to the personal data to protect it from unauthorised access or disclosure. This provision ensures that the standard of security must be maintained when the personal data is passed from the LGMA to its agent.
- That the Data Processors ensure that people processing the personal data are subject to a duty of confidence.
- That the Data Processors may only engage sub-processors with the prior consent of the LGMA and under a written contract.
- That the Data Processors assist the LGMA in providing Subject Access Requests and allowing Data Subjects to exercise their rights under the GDPR.
- Any penalties in place should the terms of the contract be broken by the Data Processor.
- That the LGMA or their agents have a right to inspect the premises of the Data Processor as to ensure compliance with the provisions of the contract.
- That the Data Processor must submit to audits and inspections by the LGMA to ensure compliance with the provisions of the contract, or by the Office of the Data Protection Commission, and provide the LGMA with whatever information it needs to ensure that they are both meeting their Article 28 obligations.
- That the Data Processor shall tell the LGMA immediately if there is a personal data breach or is asked to do something infringing the GDPR or other data protection law of the EU or a member state.
- That the Data Processor must register with the Office of the Data Protection Commission for the duration of the contract.
- That the deletion or return of the data is required upon termination or ending of the contract.

7. Retention and Disposal of Personal Data

1. Information should not be retained once the initial purpose has ceased unless there is a clear lawful basis. The LGMA recognises that personal data cannot be retained just in case the Data Subject makes a request at some time in the future. The LGMA shall not retain personal data for any purpose for longer than is necessary. The LGMA shall consider the purpose of the information, shall formalise a retention period for that type of personal data and provide adequate justification for this required retention period. After this retention period has elapsed, the personal data and associated records shall be securely deleted.

2. The retention for certain records created by the LGMA is specified under relevant regulation.
3. After the retention period has passed, the records that meet approval for destruction shall be destroyed under confidential conditions, e.g., secure shredding, comprehensive electronic deletion with certification of deletion/destruction, and in line with environmental health regulations.
4. Under the Data Protection legislation, a Data Subject has the right to request all information held in relation to them be destroyed, however this right is not absolute.
   For further details on Retention see the Data Retention Policy.

8. Personal Data Breach

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. This includes breaches that are the result of both accidental and deliberate causes. Personal data breaches can include:

- access by an unauthorised third party.
- deliberate or accidental action (or inaction) by a controller or processor.
- sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission; and
- loss of availability of personal data.

Where employees identify that a possible personal data breach has occurred, they shall report this to dataprotection@lgma.ie

An investigation shall be completed to quickly establish whether a personal data breach has occurred. Where required, additional support shall be sourced to investigate the possible breach, e.g., IT Support Services, external Data Processers, etc.

Where it is found that a personal data breach has occurred, the likelihood and severity of the resulting risk to the Data Subject's rights and freedoms shall be established.

The LGMA does not have to notify the Office of the Data Protection Commission if the breach is unlikely to result in a risk to the rights and freedoms of Data Subjects e.g., a laptop is stolen but it is protected to a high standard, e.g., appropriately encrypted.

If it is likely that there is a risk to personal data then the Office of the Data Protection Commission must be notified without undue delay, but not later than 72 hours after becoming aware of it. In case of doubt, in particular any doubt related to the adequacy of technological risk-mitigation measures, the LGMA should report the incident to the Office of the Data Protection Commission.

When reporting a breach to the Data Protection Commission, the following must be provided:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned.
- the name and contact details of a contact point where more information can be obtained.
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

The Data Subject(s) shall be notified of the personal data breach promptly by the LGMA if there is a high risk that their personal data has been obtained or used inappropriately. Supports shall be provided by the LGMA to the affected parties. The information to be provided to the Data Subjects in clear and plain language include:

- the nature of the personal data breach.
- a description of the likely consequences of the personal data breach.
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

The LGMA shall make a contact point available to the Data Subject to discuss the issue further and shall provide the Data Subject with ongoing updates relating to the investigation and close out.

In appropriate cases, the LGMA should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.

All appropriate actions shall be taken by the LGMA, to contain the breach, assess and address the potential adverse consequences for individuals and address the root cause of the breach to prevent reoccurrence.

Where the LGMA utilises a Data Processor, and this processor suffers a breach then, the Data Processer is required to inform the LGMA without undue delay as soon as it becomes aware of the breach. As the Data Controller, the LGMA is then required to notify the Data Protection Commission.

For further details on the LGMA's procedures for handling security incidents please refer to the LGMA Breach Policy.

9. Right of Access – Subject Access Requests

Under the Data Protection Acts 1988 to 2018 Data Subjects have a right to obtain a copy, clearly explained, of any information relating to them that is kept on computer or in a structured manual filing system or intended for such a system by any entity or organisation.

The LGMA recognises that Data Subjects are entitled to:

- a copy of the data the LGMA is keeping about him or her.
- know the categories of their data and the LGMA's purpose/s for processing it.
- know the identity of those to whom the LGMA discloses the data.
- know the source of the data unless it is contrary to public interest.
- know the logic involved in automated decisions.
- data held in the form of opinions, except where such opinions were given in confidence and even in such cases where the person's fundamental rights suggest that they should access the data in question it should be given.

All Subject Access Requests must be made to the LGMA at dataprotection@lgma.ie This may be made verbally or in writing, however, personal information shall never be provided to individuals over the phone.

10. Employee Education and Training

The LGMA shall identify the education and training requirements of employees to help ensure that the LGMA complies with legislation and best practice when handling Data Subject's personal information. Employees at all levels shall be adequately trained to understand the implications of losing personal data.

All reasonable measures should be taken to ensure that employees are made aware of the LGMA's data security measures and that employees are complying with them. All employees shall receive training at induction, and on a periodic basis, in accordance with their role, to ensure their awareness of the data protection requirements. The training shall include:

- their obligations in respecting and ensuring appropriate data protection within the LGMA.
- the need for data privacy.
- how to recognise data security breaches and what to do in the event of a data security breach.

All employees shall undertake annual training in data protection, confidentiality and IT/cyber security.