DATA BREACH POLICY & PROCEDURES

Revision History

Version	***Revision Date***	***Revised by***	***Section Revised***
V1	01/10/2019		
V2	20/06/22		

Document Control

Document Owner: ***Paula Prunty***	***Document No:***	***Status:*** Approved	***Date Approved:***
Security Classification: Medium	***Next Review Date:***	***Version:*** V1.0	***Department:*** Law

1 POLICY STATEMENT

Ladies Gaelic Football Association *(hereinafter referred to as **"LGFA")*** is committed to our obligations under the regulatory system and in accordance with the GDPR and maintain a robust and structured program for compliance and monitoring of our data management practices. However, we recognise that security and compliance breaches can occur, hence this policy states our intent and objectives for dealing with such incidents.

Although we understand that not all risks can be mitigated, we have procedures in place to help protect data subjects and their personal information from any risks associated with processing data. The protection and security of the personal data that we process is of paramount importance to us and we have developed data specific protocols for any breaches relating to the GDPR and the data protection laws.

2 PURPOSE

The purpose of this policy is to provide LGFA's intent, objectives and procedures regarding security and compliance breaches involving personal information. Having obligations under the GDPR, we also have a requirement to ensure that adequate procedures, controls and measures are in place and are disseminated to all those who process personal data on behalf of the LGFA, ensuring that they are aware of the protocols and reporting lines for data breaches. This policy details our processes for reporting, communicating and investigating such breaches and incidents.

3 SCOPE

This policy applies to all staff within LGFA *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with LGFA in Ireland or overseas).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

4 DATA SECURITY & BREACH REQUIREMENTS

LGFA's definition of a personal data breach is any incident of security, lack of controls, system or human failure, error or issue that leads to, or results in, the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Alongside our *'Privacy by Default"* approach to protecting data, we also have a legal, regulatory and business obligation to ensure that personal information is protected whilst being processed by LGFA. Our technical and organisational measures are detailed in our Data Protection Policy & Procedures and Information Security Policies.

We carry out information audits to ensure that all personal data processed by us is adequately and accurately identified, assessed, classified and recorded. We carry out risk assessments that assess the scope and impact of any potential data breach, both on the processing activity and the data subject. We have implemented adequate, effective and appropriate technical and organisational measures to ensure a level of security appropriate to the risks, including *(but not limited to*): -

- Pseudonymisation and encryption of personal data

- Restricted access
- Reviewing, auditing and improvement plans for the ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Disaster Recovery and Business Continuity Plans to ensure up-to-date and secure backups and the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Audit procedures and stress testing to test, assess, review and evaluate the effectiveness of all measures in compliance with the data protection regulations
- On-going data protection training programs for all employees

4.1 OBJECTIVES

- To adhere to the GDPR and Irish Data Protection laws and to have robust and adequate procedures and controls in place for identifying, investigating, reporting and recording any data breaches
- To develop and implement adequate, effective and appropriate technical and organisational measures to ensure a high level of security with regards to personal information
- To utilise information audits and risk assessments for mapping data and to reduce the risk of breaches
- To have adequate and effective risk management procedures for assessing any risks presented by processing personal information
- To ensure that any data breaches are reported to the correct regulatory bodies within the timeframes set out in any regulations, codes of practice or handbooks
- To use breach investigations and logs to assess the root cause of any breaches and to implement a full review to prevent further incidents from occurring
- To use the Data Breach Notification Form for all data breaches, regardless of severity so that any patterns in causes can be identified and corrected
- To protect customers, tenants, service users and employees; including their information and identity
- To ensure that the Data Protection Officer is involved in and notified about all data breaches and risk issues
- To ensure that the Data Protection Commission is notified of any data breach (*where applicable*) with immediate effect and at the latest, within 72 hours of LGFA having become aware of the breach.

5 DATA BREACH PROCEDURES & GUIDELINES

LGFA has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. Our procedures and guidelines for identifying, investigating and notification of breaches are detailed below. Our documented Data Breach Policy aims to mitigate the impact of any data breaches and to ensure that the correct notifications are made.

5.1 BREACH MONITORING & REPORTING

LGFA has appointed a Data Protection Officer (email - dataprotection@lgfa.ie) who is responsible for the review and investigation of any data incident involving personal information, regardless of the severity, impact or containment. Addtionally LGFA has aquired the services of GDPR for Sport as our Data Protection Consultant. LGFA has a legal obligation to report data breaches to the Data Protection Commissioner within 72 of being made aware of the incident. It is therefore imperative that any data incident must be reported to the DPO with immediate effect, whereby the procedures detailed in this policy are followed.

All data incidents will be investigated, even in instances where notifications and reporting are ultimately not required, and the DPO will retain a full record of all data incidents and breaches to ensure that gap and pattern analysis are available and used. Where a system or process failure has given rise to a notifiable data breach, revision to any such process is required.

5.2 DATA INCIDENT PROCEDURES

5.2.1 IDENTIFICATION OF AN INCIDENT

As soon as a data incident has been identified, it must be reported to the Data Protection Officer immediately so that breach investigation procedures can be initiated and followed without delay.

Reporting incidents in full and with immediate effect is essential to the compliant functioning of the LGFA and is not about apportioning blame. These procedures are for the protection of the LGFA, its staff, members, service users, members of the public and third parties and are of the utmost importance for legal and regulatory compliance.

As soon as an incident has been reported to the DPO, measures must be taken to contain the impact. Such measures are not in the scope of this document due to the vast nature of such incidents and the variety of measures to be taken. However, the aim of any such measures should be to stop any further risk/breach to the organisation, member, service user, third-party, system or data prior to investigation and reporting. The measures taken are noted on the incident form in all cases.

5.2.2 INCIDENT RECORDING

LGFA utilises an Incident Recording Form for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged and are reviewed against existing records to ascertain patterns or reoccurrences.

In all cases of data incidents, the Data Protection Officer is responsible for carrying out a full investigation, appointing the relevant staff to contain the impact of the incident, undertaking an analysis of the incident and, where necessary, making any relevant and legal notifications.

A full investigation is conducted and recorded on the Incident Recording Form, with the outcome being communicated to management. A copy of the completed incident form is filed for audit and documentation purposes.

If applicable, the Data Protection Commission and the data subject(s) are notified in accordance with the GDPR requirements (*refer to section 6 of this policy*). The Data Protection Commission protocols

are to be followed and their online '***Breach Notification Form'*** should be completed and submitted. In addition, depending on the nature and extent of the incident, any individual whose data or personal information has been compromised is notified.

5.3 BREACH RISK ASSESSMENT

5.3.1 HUMAN ERROR

Where the data breach is the result of human error, an investigation into the root cause is carried out.

A review of the procedure(s) associated with the breach is conducted and a full risk assessment completed. Any identified gaps that are found to have caused/contributed to the breach are revised and risk assessed to mitigate any future occurrence of the same root cause.

If the breach was due to human error which involves an IT system or process, the DPO will request the assistance of the LGFA IT department to resolve the breach and to mitigation any future risk.

Resultant employee outcomes of such an investigation can include, but are not limited to: -

- Re-training in specific/all compliance areas
- Restriction on access to or use of certain data sets or systems
- Review of vendor due diligence assessments and protocols
- Re-assessment of compliance knowledge and understanding

5.3.2 SYSTEM ERROR

Where the data incident is the result of a system error/failure, the LGFA IT team are to work in conjunction with the DPO to assess the risk and investigate the root cause of the incident. The IT team and the DPO will work in close cooperation, with each ensuring the other is aware of any data incident involving an IT system as soon as possible.

A gap analysis is to be completed on the system(s) involved and a full review and report to be added to the Incident Recording Form.

Any identified gaps that are found to have caused/contributed to the incident are to be revised and risk assessed to mitigate and prevent any future occurrence of the same root cause. Full details of the incident should be determined and mitigating action such as the following should be taken to limit the impact of the incident: -

- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- The use of back-ups to restore lost, damaged or stolen information
- Making the building physically secure to prevent unauthorised access
- If the incident involves any entry codes or passwords, then these codes must be changed immediately and members of staff informed

5.3.3 ASSESSMENT OF RISK AND INVESTIGATION

The DPO should ascertain what information was involved in the data incident and what subsequent steps are required to remedy the situation and mitigate any further breaches.

The lead investigator should look at: -

- The type and volume of information involved
- The sensitivity or personal content of the data involved
- What protections are in place (e.*g. encryption*)?
- What happened to the information/Where is it now?
- Whether there are any wider consequences/implications to the incident

The appointed lead investigator should keep an ongoing log and clear report detailing the nature of the incident, steps taken to preserve any evidence, notes of any interviews or statements, the assessment of risk/investigation designating a notifiable Breach and any recommendations for future work/actions.

6 BREACH NOTIFICATIONS

LGFA recognises our obligation and duty to report data breaches in certain instances. All staff have been made aware of the requirement to ensure that data incidents are identified and reported to the DPO without delay, so that a timely determination of a Breach can be made.

6.1 DATA PROTECTION COMMISSION NOTIFICATION

The Data Protection Commission is to be notified of any breach where it is likely for an incident to result in a risk to the rights and freedoms of individuals. These are situations where the breach would lead to significant detrimental effects on the individual, their privacy or confidentiality.

Where applicable, the Data Protection Commission is notified of the breach no later than 72 hours after the LGFA becomes aware of it and are kept notified throughout any breach investigation, being provided with a full report, including outcomes and mitigating actions as soon as possible, and always within any specified timeframes.

If for any reason it is not possible to notify the Data Protection Commission of the breach within 72 hours, the notification will be made as soon as is feasible, accompanied by reasons for any delay. Where a breach is assessed by the DPO and deemed to be unlikely to result in a risk to the rights and freedoms of natural persons (e.g. where a lost or stolen device is encrypted), we reserve the right not to inform the Data Protection Commission in accordance with Article 33 of the GDPR.

The notification to the Data Protection Commission will contain: -

- A description of the nature of the personal data breach
- The categories and approximate number of data subjects affected
- The categories and approximate number of personal data records concerned

- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach *(including measures to mitigate its possible adverse effects)*

Incident response procedures are always followed and an investigation carried out, regardless of our notification obligations and outcomes, with reports being retained and made available to the Data Protection Commission if requested.

Where the LGFA acts in the capacity of a Data Processor, we will ensure that the respective Controller is notified of the breach without undue delay. In instances where we act in the capacity of a Data Controller using an external Data Processor, we have a written agreement in place to state that the Processor is obligated to notify us without delay after becoming aware of a personal data security incident.

6.2 DATA SUBJECT NOTIFICATION

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the DPO will communicate the circumstances of the personal data breach to the impacted data subject(s) without undue delay, in a written, clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach
- The name and contact details of our Data Protection Officer and/or any other relevant point of contact (*for obtaining further information)*
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken by the LGFA to address the personal data breach *(including measures to mitigate its possible adverse effects)*
- Suggested measures which the Data Subject might take in order to further minimise the impact of the Breach.

We reserve the right not to inform the data subject(s) of any personal data breach where we have implemented the appropriate technical and organisational measures which render the data unintelligible to any person who is not authorised to access it *(i.e. encryption, data masking, etc.*) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise.

If informing the data subject(s) of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

7 RECORD KEEPING

All records and notes taken during the identification, assessment and investigation of the data breach are recorded and authorised by the Data Protection Officer and are retained for a period of **6 years** from the date of the incident. Incident Recording Forms are to be reviewed quarterly to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

8 RESPONSIBILITIES

LGFA will ensure that all staff are provided with the time, resources and support to learn, understand and implement all procedures within this document, as well as understanding their responsibilities and the data incident reporting lines.

The Data Protection Officer is responsible for regular compliance audits and gap analysis monitoring and the subsequent reviews and action follow ups. There is a continuous audit trail of all compliance reviews and procedural amendments and feedback to ensure continuity through each process and task.