Kickboxing Ireland

Data Breach Policy 2021

Managing a Data Breach
It should be noted that a Data Breach can have serious consequences for an Organisation and for all concerned including Staff and Service Users.

Effective Management of the breach is more important than the breach itself. It is vital that immediate and proactive steps are taken by the Data Controller/ Data Processor to minimise the effects of the breach on the Data Subject or Subjects.

A Data Breach is defined under GDPR Regulations 2018 in Article 4 (12) as "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 relates to a **type of security incident. Article 4 (12) only applies where there is a Breach of Personal Data.** It means that the Data Controller ensures compliance with the principles relating to the processing of Personal Data as outlined in Article 5 of GDPR Regulations. A notable distinction is made between Security Breaches, Personal Data Breaches and Integrity Breaches they do not always follow each other.

There are three types of Personal Data Breaches as follows:

1. **Confidentiality Breach**
   This occurs where there is inappropriate access control allowing unauthorised use. In the context of the cloud-based technology services, that we offer, one of the biggest confidentiality breaches is hacking or cyber attacks. Examples of such attacks are:

   Hacking / Cyber Attack
   - Infection by ransomware which would encrypt the Controller's or the Processor's Data until a ransom is paid
   - Obtaining information and data by deception
   - Misaddressing of emails / faxes / human error
   - Sending material to the incorrect party
   - Leaving Data on a screen in the business premises when and where it can be seen by unauthorised third parties.
   - Wilful / malicious Data breaches by employees
   - Identity theft
   - If an individual receives an email impersonating a particular Data Controller/ Data Processor which contains Personal Data relating to the Controllers/ Processors

This list is not exhaustive, there may be other instances and scenarios where there is an unauthorised or accidental disclosure of or access to Personal Data.

2. **Availability Breach**
   This occurs where there is accidental or unauthorised loss of access or destruction of Personal Data.

3. **Integrity Breach**
This occurs where there is an unauthorised or accidental alternation of Personal Data.

There are a number of typical examples of Data Breaches:

- Loss or theft of Data equipment on which Data is stored.
- Loss of unencrypted Data, where it is not possible to ascertain whether unauthorised persons have gained access to it.
- Loss of the Data Controllers'/ Data Processors' customer database where it is lost or stolen, loss or theft of documents / folders/ files stored on the cloud.
- A breach of security leading to the accidental or unlawful destruction or loss of the Data.
- Unforeseen circumstances such as a flood or fire which destroys information which could lead to Data Breaches, these events may effect an individual or individuals.

What to do in the event of a Data Breach?

1. In the event of a Data Breach staff should contact the Data Protection Officer, Shane Culleton, who can be contacted via email at shaneculleton1978@gmail.com , telephone 086 3399287 or in the event that the Data Protection Officer is unavailable or on leave, please contact our President Roy Baker on 087 6775614.

   Notification in the event of a Data Breach **must be made immediately** to the Data Protection Officer , Shane Culleton at shaneculleton1978@gmail.com or to our President Roy Baker at roy.baker@sse.com

2. A report must be submitted by the member of staff and the report must contain the following information:

   (a) The date and time of the Breach
   (b) How the Breach occurred
   (c) How the Breach was detected
   (d) Number of individuals effected by the breach (potentially)
   (e) Type of Personal Data disclosed e.g. name, address, sensitive information, Video, vehicle registration plates, photos etc
   (f) Whether or not the Data has been secured / retrieved
   (g) Measures to be implemented to mitigate the risk of reoccurrence of a similar type of incident in the future
   (h) What lessons have been learnt from the events

3. Data Breach Notification is **Mandatory and must be made by the DPC within 72 hours after** having become aware to the Supervisory Authority. If notification is not made within the **72-hour period reasons for the delay must accompany the notification when it is made.** In the event of a Data Breach the Staff Member shall complete a Data Breach Incident Report Form attached (Appendix 1).

4.Details of the Data Breach are completed by the Data Protection Officer on foot of the report from the Staff Member. The Breach Notification Form is completed and the Breach is logged in accordance with Article 33 of the GDPR Regulations 2018.

The Data Protection Office provides guidance for the completion of the Data Breach Notification Form, available here https://forms.dataprotection.ie/telecom-isp-provider-data-breach

5. Where the Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Natural Person, the Breach must be reported to the Office of the Data Protection Commission under Article 34 (1) of the GDPR Regulations 2018. The minimum sanction and containment of any harm/ distress to the Data Subject (s) is a vital aspect in dealing with any Data Breach.

6. There are instances where a Data Breach does not have to be reported to the Supervisory Authority, this would arise if there is no harm to the Data Subject but the incident must still be lodged using the Data Breach Log. The logging of the incident should contain a report as to how the Breach occurred, how it was dealt with, an account of remedial measures to contain and minimise the effects of the Breach (Appendix 1)

The log should also contain details of ongoing and future measures to avoid reoccurrence of a similar event.

The retention and maintenance of the Breach Log is to comply with GDPR Regulations 2018 and for Data Audit purposes. A practical example of where a Data Breach occurs which needs to be logged and there is no harm to the Data Subject, in these instances the **Data Breach does not need to be reported to the Supervisory Authority examples of this are as follows:**

(a) Where Data on a computer / manual information is lost or mislaid and the material is recovered with no harm to the Data Subject or if the device is encrypted.
(b) If a data file is sent to the wrong place or to the wrong person in error and by mistake and the information is retrieved and there is no harm to the Data Subject.

It is the Policy of Kickboxing Ireland to manage any Data Breach that occurs and to assist and support staff in relation to them, while at the same time fully complying with Data Protection laws.

Article 29 Work Party Guidelines outlines and provide a number of examples of Personal Data Breaches and they provide a number of useful guides pertaining to notification requirements to the Office of the Data Commissioner. The distinction is clearly made between Data Breaches if there is harm, distress or a risk to the freedom of the natural person i.e. the Data Subject. **The Mandatory Requirement is to report the Breach to the Office of the Data Commissioner which has to be complied with.** If there is no harm to the Data Subject (s) then the Breach does not have to be reported but logged.

7. The Data Processor's and Staff can report a Data Breach by completing the Data Breach Incident Form to the Data Protection Officer at shaneculleton1978@gmail.comas outlined. This Policy should be read in conjunction with Kickboxing Ireland's Data Protection Policy.

Articles 33 and 34 of the General Data Protection Regulation 2016/679 state that reporting of breaches of personal data to the Data Protection Commission and to the affected data subjects are mandatory where the breach poses a high risk to data subjects.

Where reporting is required it must be done without delay and no later than **72 hours** after having become aware of it.

This obligation should be reflected in appropriate contracts signed between Data Controllers and Data Processors also, so that a Data Processor processing on behalf of the Data Controllers will know to react immediately to any data breach that occurs through their processing, and report same to the DPO, Shane Culleton, as soon as they become aware. This obligation should also be reflected in contracts between Data Processors and Sub-Processors, and the same criteria followed such a breach occur through their processing.

Any employees who become aware of a data or a potential data breach are to report the breach to Shane Culleton or Roy Baker of Kickboxing Ireland , who are responsible for data protection as soon as they become aware. The employee reporting the breach and their manager will cooperate fully with the responsible person in complying with the below steps and with any queries from the Data Protection Commission which may follow.

Where it is determined together by management and by the person responsible for data protection, that the breach should be reported, the responsible person will notify the Data Protection Commission, on behalf of Kickboxing Ireland as the Data Processor, as follows:

a) Describe the nature of the breach, including the categories and approximate number of data subjects concerned, and the categories and approximate number of data records concerned.

b) Provide the Data Protection Commission with the name and contact details of the Data Protection Responsible Person at Kickboxing Ireland from whom more information can be obtained if required.

c) Describe the likely consequences of the data breach.

d) Describe the measures taken, or proposed to be taken by Shane Culleton at Kickboxing Ireland of the data breach, including where appropriate, measure to mitigate its possible adverse effects.

Appendix 1: Data Breach Incident Report Form

Date of Incident:

_____

Details of Incident. Please submit full report:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Were matters resolved within 72 hours of the incident being reported:

_____

_____

_____

_____

If matters were not resolved in 72 hours, please outline why?

_____

_____

_____

Who was and is affected by the data breach?

What measures are and have been taken to protect the rights and interests of the data subjects?

What type of sensitive data was disclosed?

Was the breach reported to the data subject?

Was there a need to do so or not?

DPRN Sign off: _____

Date: _____