BOWLSWALES

GDPR - PERSONAL DATA BREACH NOTIFICIATION PROCEDURE

INTRODUCTION

1. The General Data Protection Regulation ('GDPR') introduces mandatory obligations on organisations which process and exercise control over personal data (known as "controllers") to notify personal data breaches to the relevant supervisory authority[1] (for our purposes, this will usually be the Information Commissioner's Office ("ICO")) and individual data subjects.

2. BowlsWales is a controller under the GDPR and is, therefore, subject to these mandatory breach notification obligations.

3. Failure to notify personal data breaches to relevant supervisory authorities and data subjects in accordance with the requirements of the GDPR may lead to fines of up to €10million or 2% of annual global turnover (whichever is the highest).

4. Whilst BowlsWales takes the safety and security of the personal data that we process extremely seriously and has in place technical and organisational measures designed to protect the security of personal data, it is not possible to eradicate entirely the risk of a personal data breach.

5. The purpose of this procedure is, therefore, to set out how BowlsWales will deal with a personal data breach under the GDPR. Adhering to this procedure will help ensure that:

   (a) personal data breaches are dealt with appropriately, effectively and efficiently; and

   (b) we meet the requirements of the GDPR.

6. All members of staff are required to familiarise themselves with and follow the procedures set out in this document in the event of a personal data breach. Failure to do so may result in disciplinary action being taken against you by BowlsWales.

WHAT IS A PERSONAL DATA BREACH?

7. The GDPR defines a personal data breach 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*".

[1] These are referred to as "supervisory authorities" in the GDPR.

8. You can find out more information about what constitutes personal data by looking at our Privacy Policy which can be found at www.bowlswales.com

9. The following are all examples of personal data breaches:

   (a) personal data is accidentally lost or deleted by an employee;

   (b) personal data is corrupted;

   (c) if someone accesses personal data or passes it on without proper authorisation;

   (d) there is a network intrusion by a third party (e.g. a hacking incident or another type of cyber security attack);

   (e) data or equipment on which personal data is stored, is lost or stolen;

   (f) inadequate security controls (such as weak passwords) result in an authorised person gaining access to an IT system which includes personal data;

   (g) human error resulting in information being sent to the incorrect recipient;

   (h) personal data is destroyed by unforeseen circumstances such as fire or flood;

   (i) a 'blagging' offence takes place where information is obtained by deception.

WHAT DOES THE GDPR REQUIRE IF THERE IS A PERSONAL DATA BREACH?

10. Notification to the ICO and/or data subjects

10.1 If there is a personal data breach:

   (a) there is a requirement to notify the ICO unless the breach is unlikely to result in a risk to the rights and freedoms of individuals; and

   (b) there is a requirement to notify individual data subjects where the personal data breach is likely to result in a high risk to the rights and freedoms of individuals.

11. Timescales

Notifying the ICO

11.1 Where a personal data breach requires notification to the ICO, the GDPR requires that this takes place **without undue delay** and, where feasible, no later than **72 hours** after an organisation becomes aware of the personal data breach.

11.2 The clock starts ticking from the time an organisation has enough information to confirm that there has been a breach and provide some basic facts. This is the case even if it is not possible to provide full details at this time. Additional information may be provided to the ICO in stages provided this is done without undue further delay.

11.3 If the initial notification is not made within 72 hours, it is necessary to inform the ICO of the reasons for the delay in reporting the breach.

Notifying individual data subjects

11.4 Where a personal data breach requires notification to individual data subjects, the GDPR requires that this takes place **without undue delay**, whilst there is no overall deadline, communications to data subjects should be made as soon as reasonably feasible and in close co-operation with the ICO.

12. Keeping a record of personal data breaches

12.1 Irrespective of whether there is a duty to notify the ICO or individual data subjects, the GDPR requires BowlsWales to keep a record of personal data breaches.

12.2 The record must include:

(a) the facts relating to the breach;

(b) the effect of the breach;

(c) confirmation of any remedial action taken.

12.3 The ICO may require sight of the record to verify an organisation's compliance with the GDPR.

BOWLSWALES COMPLIANCE OFFICER

13. The person within BowlsWales with overall responsibility for dealing with personal data breaches is the General Manager, who is responsible for:

a) Assessing and containing any personal data breach;

b) Investigating the breach;

c) Ensuring the GDPR's record keeping requirements are met;

d) Making any necessary notifications under the GDPR;

e) Evaluating lessons learned; and

f) Implementing any additional security or procedural measures deemed necessary to minimise the risk of a similar personal data breach occurring and/or to improve our methods of handling personal data breaches.

14. Our Compliance Officer may require the assistance of other members of staff from time to time. For example, those who are involved in a personal data breach and/or who have the expertise necessary to assist with the containment, assessment or evaluation of or recovery from a personal data breach.

THE STEPS THAT WILL BE TAKEN BY BOWLSWALES TO ENSURE THE EFFECTIVE AND EFFICIENT MANAGEMENT OF PERSONAL BREACHES

Note: In view of the potentially serious consequences (both for data subjects and BowlsWales that may flow from failing to notify a personal data breach in accordance with the requirements of the GDPR, BowlsWales requires that all members of staff act responsibly and quickly if they become aware of a personal data breach. Failing to do so, may amount to a disciplinary offence.

15. Step 1 – The logging of a personal data breach

15.1 Upon becoming aware of any personal data breach, a member of staff must take immediate action to bring the breach to the attention of the General Manager or, if he or she is unavailable, our Compliance Officer in person or by telephone. You can email Sophie.hancocks@bowlswales.com. **ALL personal data breaches must be reported in this way by any members of staff who become aware of a personal data breach. It is not for members of staff to assess and determine the potential seriousness of any personal data breach. That is the role of the Compliance Officer.**

15.2 Immediately after the member of staff has brought the personal data breach to the attention of the Compliance Officer, the member of staff must officially log the breach by filling out Part 1 of the **Personal Data Breach Record Form**, set out in Appendix 1 of this procedure, and emailing the form to The General Manager.

15.3 The Compliance Officer will be responsible for completing Part 2 of the Personal Data Breach Record Form in due course, with the assistance of the member of staff who logged the breach if necessary. The completed Personal Data Breach Record Form shall form the basis

BowlsWales' compliance with the requirement under the GDPR that organisation's keep records of all personal data breaches and shall be filed in the GDPR file with the General Manager and copies retained.

15.4 All correspondence or other documentation relating to the breach should be retained and passed to the General Manager.

16. Step 2 - Containment and recovery of data

16.1 Once the Compliance Officer has been made aware of a data security breach they will take the following initial steps:

(a) identifying who within BowlsWales needs to be made aware of the breach and informing them of what they are expected to do to assist in the containment exercise;

(b) identifying and implementing, with the assistance of such other members of staff as may be required, such steps as may be necessary to contain the breach. Such steps may include, for example, remotely wiping a laptop or mobile telephone, isolating or closing a compromised section of the computer network, retrieving a lost piece of equipment or changing passwords and/or access codes;

(c) establishing whether anything can be done to recover any loss of data or to limit the damage the breach may cause;

(d) determining whether police and/or BowlsWales' insurers should be notified of the personal data breach and, if deemed appropriate, making such notification.

17. Step 3 - Assessing the risks

17.1 The next step that will be taken by the Compliance Officer is to assess the level of risk to the rights and freedoms of individuals that is likely to result from the breach for the purposes of:

(a) determining whether the breach should be notified to the ICO and/or individual data subjects (see paragraph 21);

(b) notifying any other regulatory bodies]; and

(c) determining what other steps need to be taken to deal with the personal data breach.

17.2 This will require an assessment of the potential adverse consequences of the personal data breach for individuals. For example:

(a) some personal data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job and will not, therefore, require notification to the

ICO or individuals. For example, where a laptop is damaged but its files were backed up and can be recovered, albeit at some cost to the business;

(b) other types of incidents may lead to significant risks. For example, the theft of a customer database which may be used to commit identity fraud.

17.3 To assess the risks posed by a personal data breach and the appropriate response, Compliance Officer is required to complete the **Risk Assessment Checklist** set out in Appendix 2.

17.4 In doing so, the Compliance Officer shall have regard to:

(a) the timescales relating to the notification of personal data breaches detailed in paragraphs 11.1 – 11.3 above; and

(b) the guidelines relating to when notifications may need to be made to the ICO or individual data subjects set out in Appendix 3 (the "**Notification Guidelines**").

18. Step 4 - Notification of a personal data breach

18.1 As stated above:

(a) the ICO must be notified of any personal data breach unless it is **unlikely to result in a risk** to the rights and freedoms of individuals.

(b) individual data subjects must be notified of any personal data breach where the breach is likely to result in a **high risk** to the rights and freedoms of individuals.

18.2 Completion of the **Risk Assessment Checklist** and reference to the **Notification Guidelines** will assist the Compliance Officer to decide whether a personal data breach does or does not need to be notified to the ICO and individual data subjects.

Notifying the ICO

18.3 Where the Compliance Officer comes to the conclusion that a personal data breach requires notification to the ICO, the Compliance Officer shall ensure that the timing of the notification meets the requirements set out in paragraphs 11.1 – 11.3 above.

18.4 In relation to the content of the notification, the Compliance Officer shall ensure that the information provided includes the minimum information required by the GDPR, which is as follows:

(a) the nature of the personal data breach including where possible, the categories and approximate number of data subjects and personal data records concerned;

(b) the name and contact details for BowlsWales;

(c) the likely consequences of the personal data breach;

(d) the measures taken or proposed to be taken to address the personal data breach, including any measures to mitigate its possible adverse effects.

Notifying individual data subjects

Exceptions relating to notification of individual data subjects

18.5 Certain exceptions apply to the mandatory obligation to notify personal data breaches to individual data subjects.

18.6 These are:

(a) if the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular, those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) if the controller has taken subsequent measures to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;

(c) if notification would require disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

18.7 The Compliance Officer will determine whether an exemption relating to the notification of individual data subjects applies.

18.8 Where the Compliance Officer comes to the conclusion that a personal data breach requires notification to the individual data subjects, the Compliance Officer shall ensure that the timing of such notification meets the requirements set out in paragraph 11.4 above.

18.9 In relation to the content of the notification, the Compliance Officer, shall ensure that the communication includes the following:

(a) the name and contact details of our Compliance officer;

(b) a summary of the incident causing the breach;

(c) the estimated date of the incident;

(d) the nature and content of the personal data concerned (and in particular whether it included any of the special categories of personal or any financial information);

(e) the likely consequences of the breach on the individual concerned (and in particular, whether there is a risk of identity theft or fraud, physical harm or damage to reputation;

(f) the measures taken by us to address the breach; and

(g) the measures that the individual could take to mitigate the adverse consequences of the breach and what we can do to assist them;

(h) a helpline number and/or email address the individual can use to contact us.

18.10 The Compliance Officer shall also ensure that the means of communication is prompt and secure, in clear and plain language and that it is a specific message concerning the breach. It should not be combined with a communication on another topic.

Other notifications

18.11 The Compliance Officer shall make such other notifications as may be necessary in accordance with any applicable rules.

18.12 Where a notification is made to either the ICO or individual data subjects, the Compliance Officer shall be responsible providing such ongoing assistance to the ICO or such individual data subjects as may be necessary or desirable in the circumstances. The Compliance Officer shall liaise with the Board prior to taking any actions or steps which may have legal or reputational consequences for BowlsWales.

19. Step 5 - Evaluation and response

19.1 Once a breach has been contained, any notifications made and the immediate risks dealt with, the Compliance Officer shall:

(a) investigate fully the causes of the personal data breach, in particular to identify whether any changes to our policies and procedures are necessary in order to reduce the likelihood of such a breach reoccurring; and

(b) evaluate the effectiveness of our response to the personal data breach, with a view to implementing such changes to our procedures and/or chain of responsibility as may be necessary to ensure that any future personal data breaches are properly handled.

19.2 The Compliance Officer shall ensure that the findings are recorded in a report. In the case of personal data breaches, which require notification to the ICO and/or data subjects, the report will be presented to the Board, which shall agree with the Compliance Officer the actions to be taken. In the case of other personal data breaches the Compliance Officer will determine what actions need to be taken to remedy any issues and shall file a copy of the report in the GDPR file along with the related Data Breach Record Form.

If LEGAL ADVICE IS NEEDED?

20. In some circumstances, it may be clear that notification needs to be made to the ICO or individual data subjects and what the content of that notification needs to include.

21. At other times, this may not be so clear. Where there is such uncertainty, consider referring the matter to our internal legal Director

REVIEW OF THIS PROCEDURE

22. This procedure will be reviewed annually by the Board and the Compliance Officer .

23. Any questions regarding this procedure should be addressed to the Compliance Officer.

RENTENTION OF DOCUMENTS

24. The record of any personal data breach together with all correspondence or other documentation relating to the breach will be kept for the period stipulated in BowlsWales Document Retention Policy.

APPENDIX 1

Personal Data Breach Record Form

PART 1 - To be completed by the member of staff who becomes/is made aware of a personal data breach	
Name	
Department	
Date and time breach occurred	
When and where did the breach occur?	
[Data Protection Officer/other] notified? Y/N	
Date, time and method of notification	
What type of personal data breach has occurred?	
Personal data has been accidentally lost or deleted by an employee.	
Personal data has been corrupted.	
Someone accesses personal data or passes it on without proper authorisation.	
A network intrusion by a third party (e.g. a hacking incident or another type of cyber security attack).	
Data or equipment on which personal data is stored has been lost or stolen.	
Inadequate security controls (such as weak passwords) result in an authorised person gaining access to an IT system which includes personal data.	
Human error resulting in information being sent to the incorrect recipient.	
Personal data is destroyed by unforeseen circumstances such as fire or flood.	
'Blagging' offences where information is obtained by deceiving the organisation who holds it.	

Other (please specify)	
What type of personal data is involved?	
Is any confidential or special category data involved in the breach e.g. medical/health information, financial information or personnel data? If so what?	
What is the approximate number of individuals whose personal data are involved in the breach?	
Details of any individuals or organisations involved in the breach	
Details of individuals or organisations who are aware of the breach, including details of when and how they became aware.	

Part 2 - For completion by the Compliance Officer
The potential effect of the breach *(e.g. potential loss of customer personal data including… however laptop reported lost immediately, password protected and data encrypted, hard drive can be wiped remotely – effect of personal data breach minimal)*
The potential cause of the breach
Confirmation of any remedial action taken *(e.g. hard drive wiped remotely within 6 hours of laptop reported as lost)*

APPENDIX 2

Personal Data Breach Risk Assessment Checklist

What type of data is involved?	
Did the data include special category data (formerly sensitive personal data) e.g. health information?	
Did the data include data that was confidential or which could be used to commit fraud or identity theft (e.g. bank details)?	
What could the data tell a third party about the individual?	
When did the personal data breach occur?	
What was the time lag between the personal data breach occurring and the discovery of the personal data breach?	
If data has been lost or stolen, are there any protections in place such as encryption?	
If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relates?	

The measures taken or proposed to be taken to address the personal data breach, including any measures to mitigate its possible adverse effects.	
Assessment of whether the personal data breach should be notified to the ICO.	
Assessment of whether the personal data breach should be notified to individual data subjects.	

APPENDIX 3

Guidance relating to notification of personal data breaches to the ICO and individual data subjects

Note: Limited guidance is currently available as to the thresholds for notification to the ICO and individual data subjects. This document will be updated as and when further guidance becomes available.

NOTIFICATION TO THE ICO

- The recitals to the GDPR suggest any personal data breach which is likely to result in physical, material or non-material damage to natural persons, such as:
    - loss of control over their personal data;
    - limitation of their rights;
    - discrimination;
    - identity theft or fraud;
    - financial loss;
    - unauthorised reversal of pseudonymisation;
    - damage to reputation;
    - loss of confidentiality of personal data protected by professional secrecy; or
    - any other significant economic or social disadvantage to the natural person concerned

  should be notified to the ICO.

- ICO guidance on the GDPR states that, in order to assess whether it is necessary to notify the ICO of a personal data breach, organisations should consider whether, if any addressed, the breach is likely to have a significant detrimental effect on individual, such as:
    - discrimination;
    - damage to reputation;
    - financial loss;
    - loss of confidentiality; or

- any other significant economic or social disadvantage.

- If any personal data breach is likely to result in any of the consequences listed above, notification to the ICO should be made.

- If the personal data concerned was encrypted, a decision will need to be made as to the likelihood of decryption. If we can be confident that the personal data concerned remains secure, notification to the ICO may not be required. However, any such decision needs to take into account the potential risks if the personal data were to become accessible to third parties.

NOTIFICATION TO INDIVIDUAL DATA SUBJECTS

- There is currently even less guidance as to when a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects and therefore require notification of those concerned directly.

- It is clear, however, that a "high risk" means that the threshold for notifying individuals is higher than for notifying the ICO.

- It is our view that the following data breaches should be treated as "high risk":

    - The personal data concerned reveals the identify of vulnerable persons, including children;

    - The personal data concerned falls into the special categories of personal data set out in Article 9 of the GDPR;

    - The breach gives rise to a risk to individuals of financial loss, fraud or identity theft;

    - There is a high likelihood of damage to reputation or discrimination;

    - It is likely that, if the personal data entered the public domain, the individuals concerned would suffer significant distress.

- Bear in mind, however, that the requirement to notify individual data subjects will not apply where any of the exemptions set out in paragraph 21.6 above apply.