Procedure for Processing Personal Data for the Office of the Press Ombudsman and Press Council of Ireland (PCI-DP-02)

1. Introduction

1.1 In line with the Office's commitment to ensuring that the personal data and privacy of those using its services is protected as required by the General Data Protection Regulation and the Data Protection Act 1988-2018, the Office has adopted a procedure for processing personal data.

1.2 All staff of the Office are required to familiarise themselves with this document and also with our ***Data Protection Policy (PCI-DP-01)*.**

Application and Awareness

1.2 All staff are required to follow the procedure and failure to do so may in some instances be regarded as a disciplinary matter. Staff will receive regular training which is mandatory. Staff are required to inform the officer responsible for data protection of any instances of non-compliance with the procedure of which they become aware.

2. General security

2.1 Access to the premises of the Office of the Press Ombudsman involves a double locked front door and there is a fully monitored alarm system covering all windows and doors. The offices have a private alarm system operated by a password. In the event of the alarm being activated a management company is automatically alerted. There is no public access to the offices other than by appointment. All staff are obliged to lock doors and set the alarm on leaving the offices.

2.2 Staff maintain a strict confidentiality policy when dealing with personal data.

- Personal data is only shared internally and externally where necessary for the purpose of performing the functions of the Office.
- Staff verify that persons calling the office by phone positively identify themselves as the person whose case is being processed and never reveal personal information about complainants to others.
- Care is taken to ensure that visitors to the office are not left alone in the office and do not have sight of any confidential documents.
- Discretion is exercised when taking calls when a visitor is present.
- Hard copy data is securely stored in locked cabinets, and personal data is put away when not in use.
- Documents containing personal data are only taken out of the premises of the Office when absolutely necessary. They must be treated with extreme care and never left unattended.
- The Office uses a company which guarantees secure and confidential disposal for all documents containing personal data. Documents are disposed of using a confidential disposal facility.. Office shredders are used for day-to-day disposal.
- Sensitive documents are sent if required using registered post or by approved courier

companies and full addresses with Eircodes are carefully checked.

3. IT Security

3.1 All staff PCs, laptops and mobiles are encrypted via Microsoft 365 Business Premium and MS Office Suite.

3.2 The Office uses multi factor authentication to protect access to our systems which are also protected by the AV Defender anti-virus suite to protect against Viruses, Malware and Spyware.

3.3 Our IT providers use Intune software to deploy Mobile Device Management, remote wipe and hard drive encryption. GeoIP blocking is configured as required

3.4 Our primary means of communication with those whose personal data is processed is email and emails are encrypted. Our IT providers monitor emails to isolate those which are fraudulent and dangerous attachments are blocked and quarantined. Emails are not set to forward to external email systems.

3.5 Emails from the Office contain a notice as follows: "The information transmitted by this email is intended only for the person or entity to which it is addressed. This email may contain proprietary, business-confidential and/or privileged material. If you are not the intended recipient of this message, be aware that any use, review, retransmission, distribution, or reproduction of any information in or with this email is strictly prohibited. If you received this in error, please advise the sender and delete the material from all computers and other devices."

3.6 Security practices:

Staff are instructed to:

- Log off and lock all PCs and laptops when unattended
- Not use personal devices for work purposes and not to use work devices for personal purposes
- Not install software on devices owned by the Office without proper authority
- Not to use unsecured wireless networks when processing personal data
- Take care when working remotely that no data is visible or accessible to others
- Store equipment securely when used outside of the premises and never leave it unattended
- Report any loss or theft of equipment including phones, USB sticks, hard-drives or laptops immediately to the relevant Officer in line with our Data Protection Policy.

All redundant equipment is securely disposed of by a designated company personal data having first been deleted.

In the event of a data breach our IT provider offers a fast response service and unlimited telephone support.

4. Data Retention Policy

4.1 Personal data related to complaints is retained for 7 years from the date of the complaint. If at the end of that period that personal data is part of a formal decision of the Press Ombudsman or an appeal decision by the Press Council, some elements of the data may have been published (usually names unless anonymity has been requested). Other data held in hard copy format and stored on the Office's database are deleted. Personal data in relation to complaints which did not lead to either conciliated resolutions or formal decisions by the Office are deleted after 7 years.

Statistical information derived from cases dealt with by the Office is retained but does not contain personal data.

5. Breaches

5.1 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."*

5.2 While the Office makes all reasonable efforts to protect personal data and confidential information from unauthorized access, use, disclosure, deletion, destruction, damage or removal the possibility cannot be ruled out that the security of data may be breached.

5.3 Breaches may occur due to:

- Loss or theft of data or equipment on which data is stored
- Failure of access controls leading to unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as flood or fire
- A hacking or phishing attack
- Access to data obtained by deception.

5.4 All staff and members of the Press Council must, upon becoming aware of a breach or a potential breach of personal data, notify the officer responsible for data protection in the Office.

5.5 The relevant officer will ensure that all necessary steps are taken to contain the breach and mitigate any potential harm.

Reporting a Breach.

5.6 The relevant officer will assess the risk level involved in any breach. If it is deemed minor i.e. the incident does not pose a risk to the privacy of an individual and can be resolved without further action, she/he will record it, including a note of why it was not deemed necessary to report it to other authorities. If the incident results in a risk to the privacy of an individual she/he will report it to the Data Protection Commission.

6. Data Subject Rights

6.1 Under GDPR Data Subjects have enhanced rights in relation to the processing of their personal data. In summary these rights are:

- To access and request a copy of your[1] personal data, which the Office holds about you
- To request your personal data is erased where it is no longer necessary or lawful for the Office to retain such data
- To request a restriction is placed on further processing of your personal data where there is a dispute in relation to the accuracy or processing
- To request that the Office corrects any personal data if it is found to be inaccurate, incomplete or out-of-date
- To object to the processing of personal data by the Office
- To request that the Office provides you with a copy of personal data that you have provided and, in certain circumstances, to transmit that data directly to another data controller.

6.2 While these rights apply to all personal data processed by a Data Controller and must be respected, the reality in the case of the Office is that only limited personal data is processed in connection with complaints and appeals and all of that data is provided by the Data Subject him or herself so (a) it is likely that request to exercise any of the rights above will be limited and (b) handling such requests will be straightforward. See PCI-DP-03 for further information on Handling Data Subject Requests.

6.3 The essential point for staff to be aware of is that, should a data subject seek to exercise one of the above rights e.g. request that his personal data be deleted after a complaint has been dealt with, the Office is required to deal with this request within one month.

[1] 'You' and 'your' refers to the Data Subject