Data Protection Policy

1. Introduction

1.1 Background.

The Office of the Press Ombudsman and the Press Council of Ireland ("the Office") is responsible for considering complaints made by members of the public concerning alleged breaches of the Press Council's Code of Practice, which sets out the standards of professional practice agreed by all publications that are members of the Press Council.

The Office is a Data Controller and strives to be fully compliant with the General Data Protection Regulation and the Data Protection Acts 1988-2018 which provide legal protections for individuals concerning the processing of their personal data, and their privacy.

1.2 Policy Aim

This document governs the processing of personal data by the Office. It sets out our legal obligations regarding data protection, and how we discharge these responsibilities in practice.

Our data protection objectives are to:

- Ensure that individuals who entrust us with their personal data feel confident that they will be handled in accordance with their rights under data protection laws;
- Ensure that all staff and service providers involved in processing personal data are competent and knowledgeable about our data protection obligations and how they apply to their specific roles within the Office;
- Enhance the Office's reputation as a reputable, trustworthy organisation which is committed to high standards of compliance and ethical behaviour;
- Minimise as far as possible the legal, financial or reputational risks to the Office that can arise from processing personal data.

2. Defining Data Protection

2.1 Personal data means information relating to an identified or identifiable living person (data subject). Such a 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, or an online identifier.

2.2 Data processing means performing operations on personal data including:

- Obtaining, recording, storing or deleting the information
- Retrieving, consulting or using the information
- Sharing the information by transmitting, disseminating or otherwise making it available

3. Compliance with Data Protection Principles

3.1 The seven principles of Data Protection require that personal data is:

- Processed in a way that is lawful, fair and transparent (*Lawfulness, Fairness and Transparency Principle*)
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes *(Purpose Limitation Principle*)
- Adequate, relevant and limited to what is necessary (*Data Minimisation Principle*)
- Accurate and kept up to date (*Accuracy Principle*)
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed *(Storage Limitation Principle*)
- Processed in a manner that ensures the appropriate security of the data (Security *and Confidentiality Principle*)
- Maintained with appropriate measures and records in place (*Accountability Principle*)

The General Data Protection Regulation requires the Office to be responsible for, and to be able to demonstrate compliance with, principle 7 ("Accountability")". Our policies and procedures are designed to ensure such compliance.

3.2: How the Office meets the requirements of the 7 principles.

Lawfulness, Fairness and Transparency: The Office processes personal data for the sole purpose of handling complaints about the press. As complainants engage with the Office voluntarily, the processing of personal data is based on the complainant's consent. On request the Office will remove a complainant's name from a complaint.

All documentation between member publications and the Press Council and the Press Ombudsman in relation to complaints, together with all statements by the Press Council and the Press Ombudsman, and publication of decisions by them, are legally privileged.

Purpose Limitation Principle: The Office processes personal data only for the purposes for which it is collected, and we ensure that the person knows that they can withdraw their consent to their data being processed by us, at any time. On request we can remove a complainant's name, and/or other potentially identifying details in relation to decisions of the Press Ombudsman and to appeals decisions by the Press Council. This can also be done retrospectively i.e. after decisions are published. We will not use or disclose personal data other than in compliance with our functions.

Data Minimisation Principle: The Office will only collect and process personal data that is necessary for the purpose of carrying out our functions. Typically, we require a person's name and email address.

Accuracy Principle: The Office endeavours to ensure that the personal data we process is accurate and kept up to date. We encourage all persons whose data we hold to inform us of any necessary changes or deletions required. We may require verification of such changes.

Storage Limitation Principle: The Office only retains personal data for the purposes for which it is processed. Personal data related to complaints is retained for 7 years from the date of the complaint. If 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 will be deleted both in terms of hard copy material and material stored on the Office's database. 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.

Security and Confidentiality Principle: The Office recognises the sensitivity of the personal data supplied to it and respects the need to maintain its confidentiality. All staff at the Press Ombudsman's office are trained in data protection and are required to adhere to our security policies. The Office ensures that:

- Access to personal data is restricted to those involved in processing it.
- Appropriate levels of IT security are applied to our systems.
- All hard copy documents are stored and disposed of securely when no longer required.

Accountability Principle: The Office takes responsibility for its compliance with the principles. We are committed to transparency and can demonstrate our best efforts at full compliance through our policy documents, evidence of staff training, and our implementation practices.

4. Our Obligations as a Data Controller

In addition to complying with the above principles of personal data management the Office recognises that it has specific obligations as a Data Controller. These obligations, and the measures taken or planned to address them, are:

4.1 Privacy Notice

The Office's Privacy Notice sets out the identity and the contact details of the controller, the contact details of the officer responsible for Data Protection, the purpose(s) and legal basis for the processing, the existence of the rights of data subjects and how to exercise them, the right to lodge a complaint with the Data Protection Commission and other information as required by law.

4.2 Record of Processing Activities (RoPA)

The Office maintains a record of personal data processing activities.

4.3 Data Breaches

The Office has extensive technical and organisational security measures in place to protect the security and confidentiality of personal data. However, the Office recognises that breaches i.e. unauthorised release of, or access to, personal data can occur. The Office understands and has procedures to assess, record and, where appropriate, notify the Data Protection Commission and/or the Data Subject.

4.4 Contracts with Data Processors

The Office contracts with external data processors to provide certain services that entail the processing of personal data e.g. IT systems and services.

The Office assesses potential service providers carefully and engages only processors who have measures in place to process personal data appropriately on our behalf. All processing of personal data is subject to having a Data Processing Agreement in place.

4.5 Data Subject Rights

The Office understands and upholds the rights of Data Subjects under Data Protection Law and has arrangements in place to ensure that these rights are understood by staff who process personal data and to respond to requests in a timely fashion.

4.6 Data Protection Impact Assessment

Where the Office processes, or is considering the processing of, personal data utilising new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, the Office carries out a Data Protection Impact Assessment (DPIA).

4.7 Data Protection Officer

The Office has assessed whether it meets the criteria requiring the appointment of a Data Protection Officer (DPO) and has concluded that a DPO is not required. Overall responsibility for data protection has been assigned to the Press Ombudsman.

4.8 Overseas Transfer

The Office is aware of its obligations to safeguard personal data transferred to third countries.

5. Monitoring

The Office carries out regular compliance monitoring with a view to ensuring that our measures and controls to protect personal data are effective and compliant.

The Press Ombudsman has overall responsibility for assessing, testing, reviewing, and improving the processes, measures and controls in place.

9. Training

The Office provides training for employees in relation to data protection, the content of which is tailored to the requirements of their roles and the extent to which they are involved in processing personal data.