



THE JUDICIAL COUNCIL DATA PROTECTION POLICY

Table of Contents

1.	Introduction	3
2.	Purpose	4
3.	Scope	4
4.	Key Definitions	4
5.	Responsibility for this Policy	6
6.	Implementation, Management, Monitoring and Review	7
7.	Policy	7
8.	Data Subject Rights	9
9.	Security of Personal Data	10
10.	Privacy by Design and Default	11
11.	General Guidelines for Staff	11
12.	Data Protection Officer	11

1. Introduction

Background

The Judicial Council was established on 17th December 2019 as an independent body pursuant to the Judicial Council Act 2019 [“the Act”]. Its objectives are to promote and maintain excellence and high standards amongst the judiciary in Ireland. The Council comprises all current members of the judiciary, while its Board is made up of 11 members being

- the Chief Justice (who is the Chairperson) and the Presidents of the Court of Appeal, High Court, Circuit Court and District Court
- one Judge from each of the Courts (Supreme Court, Court of Appeal, High Court, Circuit Court and District Court) elected by the ordinary Judges of those Courts
- a co-opted member from one of the Courts.

The Board of the Judicial Council performs the functions on behalf of the Council save those functions reserved for the Council under the Act.

The functions of the Judicial Council are set out in Section 7 of the Act. They are to promote and maintain excellence in the exercise by judges of their judicial functions, high standards of conduct among judges, continuing education of judges, respect for the independence of the judiciary and public confidence in the judiciary and in the administration of justice.

Data Protection law safeguards the rights of individuals in relation to the processing of their personal data. It confers rights on individuals as well as responsibilities on those persons processing personal data. This Policy sets out how the Council seeks to process personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work.

Although the judiciary are members of the Judicial Council, data control and processing in relation to the Council is carried out by its staff members who are all civil servants.

The EU General Data Protection Regulation (GDPR EU 2016/679) replaces the Data

Protection Directive 95/46/EC and was designed to harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy rights and to reshape the way organisations across the region approach data privacy. The GDPR came into force on 25th May 2018.

2. Purpose

This policy should be read in conjunction with other relevant Judicial Council policies and procedures. The Council may supplement or amend this policy by additional policies and guidelines from time to time.

This data protection policy is a statement of the Judicial Council's commitment to safeguard the data protection rights of individuals in accordance with Irish Data Protection and GDPR requirements.

3. Scope

The Policy covers both personal and special categories of personal data (as defined by Article 4 of the GDPR) held in relation to data subjects by the Council. The Policy applies to personal data held in both manual and automated forms.

Both categories will be equally referred to as Personal Data in this Policy, unless specifically stated otherwise. Personal data and special categories of personal data will be treated with equal care by the Council.

4. Key Definitions

The term "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that

natural person.

The term "special categories of personal data" means personal data consisting of information as to:

- The racial or ethnic origin of the data subject
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether he/she is a member of a trade union
- Their physical or mental health or condition
- Their sexual life
- Their genetic data
- Their biometric data
- Processing of personal data relating to criminal convictions and offences.

"Data processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

A "data subject" is an individual who is the subject of personal data. In terms of the Judicial Council, all members of the public, judges, employees and lay members appointed by Government are data subjects.

A "data controller" means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. "Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

A "data processor" means any person, public authority agency or other body (other than an employee of the Judicial Council) who processes the data on behalf of the Council.

Please refer to Article 4 of the GDPR for additional definitions.

5. Responsibility for this Policy

The Judicial Council is committed to compliance with all relevant EU and Irish laws in respect of personal data, and the protection of the rights and freedoms of individuals whose information it controls and processes.

The Judicial Council shall implement appropriate technical and organisational measures to ensure that processing is performed in accordance with the GDPR. Everyone who works in the Judicial Council and third parties who separately collect and or control the content and use of personal data have responsibility for ensuring personal data is collected, stored and handled appropriately. Each area that handles personal data must ensure it is handled and processed in line with this policy, best practice and data protection legislation.

Data Protection Officer (DPO)

The designation of the mandatory appointment of a Data Protection Officer (DPO) is required under Article 37 of the GDPR for all public bodies. The DPO will report to senior management level of the Judicial Council and in this capacity will carry out their functions independently.

Data Protection Unit

A Data Protection Unit is the supporting administrative and operational office that provides necessary support and assistance to the DPO in the execution of their role. In the context of the Judicial Council, the DPO carries out all of these functions.

Staff

All members of staff have a responsibility to comply with the Council's Data Protection Policy. The Data Protection Officer and senior management within the Judicial Council will

ensure all work processes comply with this policy

6. Implementation, Management, Monitoring and Review

Implementation

Implementation of this Policy is the responsibility of senior management. Senior management is responsible for the development and maintenance of a Data Retention Schedule in respect of any paper-based data or system handling personal data.

Review

This Policy will be reviewed regularly in light of any legislative or other relevant developments.

7. Policy

All processing of personal data must be conducted in accordance with the data protection principles set out in relevant legislation. Our policies and procedures are designed to ensure compliance with the following principles: -

- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”)
- Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (“purpose limitation”)
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (“data minimization”)
- Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data which is inaccurate, having regard to the purposes for which it is processed, will be erased or rectified without delay

(“accuracy”)

- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (“storage limitation”)
- Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (“integrity and confidentiality”)
- When a data breach or potential data breach is identified the Data Protection Officer and line manager is to be informed. A Data Breach Recording Form is to be completed by the person who has identified the breach. A risk assessment is to be undertaken and documented by the Data Protection Officer. The Secretary to the Judicial Council will be informed of the outcome of the risk assessment within 48 hours of the breach being identified. If the breach is determined to be of low or medium risk, no further action is necessary.
- If the data breach is determined to be high risk, the people affected are to be informed within 48 hours of the breach being identified. The Data Protection Commission must be informed of the breach within 72 hours of the breach being identified. The Commission will undertake an investigation and determine any actions which must be taken to resolve the matter. The Commission may also instruct the Judicial Council on how to ensure a similar breach does not occur again. The Council must implement any changes advised by the Commission.

8. Data Subject Rights

The Judicial Council will design and maintain appropriate policies, procedures and training to implement the following data rights of data subjects.

Right of access by the data subject

We will implement procedures to ensure that requests from data subjects for access to their personal data will be identified and fulfilled in accordance with the legislation.

Right to rectification

We are committed to holding accurate data about data subjects and will implement processes and procedures to ensure that data subjects can rectify their data where inaccuracies have been identified.

Right to erasure (right to be forgotten)

The Judicial Council processes personal data it collects because there is a statutory basis for the processing. Where we receive requests from data subjects looking to exercise their right of erasure, we will carry out an assessment of whether the data can be erased without affecting the ability of the Judicial Council to carry out its statutory functions.

Right to restriction of processing

The Judicial Council will implement and maintain appropriate procedures to assess whether a data subject's request to restrict the processing of their data can be implemented. Where the request for restriction of processing is carried out then the Council will write to the data subject to confirm the restriction has been implemented and when the restriction is lifted.

Right to data portability

The Judicial Council processes personal data it collects because there is a statutory basis for the processing. Where it has collected personal data on data subjects by consent or by contract then the data subjects have a right to receive the data in electronic format to give to another data controller. It is expected that this right will apply only to a small number of data subjects.

Right to object

Data subjects have a right to object to the processing of his or her personal data in specific circumstances. Where such an objection is received, the Council will assess each case on its

merits.

Right not to be subject to automated decision making

Data subjects have the right not to be subject to a decision based solely on automated processing, where such decisions would have a legal or significant effect concerning him or her.

Complaints

The Judicial Council will implement and maintain a process whereby data subjects will be able to contact the Data Protection Officer. The Data Protection Officer will work with the data subject to bring the complaint to a satisfactory conclusion for both parties. The data subject will be informed of their right to bring their complaint to the Data Protection Commission and be provided with their contact details.

9. Security of Personal Data

The Judicial Council will ensure the confidentiality, integrity, availability, and resilience of personal data when in use, transit and in storage. It will protect the personal data from inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing through for example

- Using appropriate security controls, technical and non-technical should be utilised to protect Judicial Council personal data
- Computer screens, printouts, files or documents displaying personal data should only be visible to authorised personnel
- Personal data held in manual (paper) files should be held securely in locked cabinets, locked rooms or rooms with restricted access.

10. Privacy by Design and Default

Following best practice, the Judicial Council will conduct Data Privacy Impact Assessments

(DPIA) on relevant projects. Any staff members working on projects involving personal data should consult with the DPO as necessary.

11. General Guidelines for Staff

- The only people able to access personal data covered by this policy should be those who need it for their work
- Personal data should not be shared informally
- The Judicial Council will provide training to employees to help them understand their responsibilities when handling data
- Employees should keep all data secure, by taking sensible precautions
- Strong passwords must be used and they should never be shared
- Personal data should not be disclosed to unauthorised people, either within the Judicial Council or externally
- Personal data should be regularly reviewed and updated if it is found to be out of date and if the personal data is no longer required action should be taken in line with the Council's Retention Policy
- Employees should request help from their line manager or the DPO if they are unsure about any aspect of the protection of personal data.

12. Data Protection Officer

The Data Protection Officer will report to senior management. The responsibilities of the Data Protection Officer will include the following:

- Act as an advocate for data protection within the Council.
- Monitor compliance with the relevant data protection legislation.
- Ensure this data protection policy is reviewed and updated on a regular basis.
- Liaise with senior management to ensure that the Council provides appropriate data protection training and advice for all staff members.
- Provide advice where requested as regards data protection impact assessments and monitoring that such assessments are completed to an appropriate standard.

- Provide advice on data protection matters to colleagues.
- Respond to individuals who wish to know what data is being held on them by the Council.
- Engage with senior management to ensure that appropriate data processing agreements are put in place with third parties that handle the Council's data and ensuring that reviews of the agreements are carried out on a regular basis.
- - Monitor the record of data processing activity (ROPA) to ensure it is updated regularly.
- Act as a contact point and provide cooperation with the Data Protection Commission

The Council has appointed an internal Data Protection Officer whose contact information is as follows:

name: Katherine Meier

email: info@judicialcouncil.ie

by post: Data Protection Unit,

Judicial Council,

Green Street Courthouse

Dublin 7, D07 W568