Irish Architecture Foundation

Irish Architecture Foundation
Data Protection Policy

Last updated 27 March 2018

Definitions
Data Controller means Irish Architecture Foundation.
GDPR means the General Data Protection Regulation.
Responsible Person means Donna Carroll, Relationship & Communications Officer.
Register of Systems means a register of all systems or contexts in which personal data is processed by the Data Controller.

1. Data protection principles
The Data Controller is committed to processing data in accordance with its responsibilities under the GDPR.
Article 5 of the GDPR requires that personal data will be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. 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 will not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. 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 subject to implementation of

the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. 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.

2. General provisions

a. This policy applies to all personal data processed by the Data Controller.
b. The Responsible Person will take responsibility for the Data Controller's ongoing compliance with this policy.
c. This policy will be reviewed at least annually.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Data Controller will maintain a Register of Systems.
b. The Register of Systems will be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the Data Controller will be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the Data Controller must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests.
b. The Data Controller will note the appropriate lawful basis in the Register of Systems.
c. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent will be kept with the personal data.
d. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Data Controller's systems.

5. Data minimisation

The Data Controller will ensure on an ongoing basis that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

6. Accuracy

a. The Data Controller will take reasonable steps on an ongoing basis to ensure personal data is accurate.
b. Where necessary for the lawful basis on which data is processed, steps will be put in place to ensure that personal data is kept up to date.

7. Archiving / removal

a. To ensure that personal data is kept for no longer than necessary, the Data Controller will put in place an archiving policy for each area in which personal data is processed and review this process annually.
b. The archiving policy will consider what data should/must be retained, for how long, and why.

8. Security

a. The Data Controller will ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. Access to personal data will be limited to personnel who need access and appropriate security will be in place to avoid unauthorised sharing of information.
c. When personal data is deleted this should be done safely such that the data is irrecoverable.
d. Appropriate back-up and disaster recovery solutions will be in place.

9. Access requests

A data subject (someone whose data is held by the Data Controller) has the right to request access to, a change in, or removal of their data, subject to a number of criteria. A data subject can request access to their data in writing (or by email) and the Responsible Person will provide the actual personal data requested plus the following within one month of the request:

a. The purposes for processing the data.
b. The categories of personal data concerned.
c. To whom the data has been or will be disclosed.
d. Whether the data has been or will be transferred outside of the EU.
e. The period for which the data will be stored, or the criteria to be used to determine retention periods.
f. The right to make a complaint to the Data Protection Commissioner.
g. The right to request rectification or deletion of the data.

10. Access requests — restrictions and exemptions

The following are situations in which the Data Controller will not comply with a data access request:

a. Where the requester is involved in a claim against an organisation, seeking compensation, and the information reveals details of the organisation's decision process in relation to their claim.
b. If the information is held for statistical purposes, is not shared with any other person or organisation and cannot be identified as belonging to any particular individual.
c. If releasing the data would mean that personal data about another individual would be unfairly disclosed. (Personal data may be released in redacted form so as to protect the other individual's data.)
d. Where the data being sought involves personal opinions that have been expressed by another individual. Specifically, if the opinion was given in confidence, and it can be proven that the person providing the opinion at the time did so in the expectation of

confidence, it does not have to be released. (If the opinion was given as part of regular business communications, does not involve personal opinions, and was given without the expectation of confidentiality, it should be released.)

e. If the personal data requested is impossible to supply, or supplying it would be extremely difficult (disproportionate effort).
f. If the personal data has already been supplied in accordance with an access request, but identical requests continue to be made (unless new data has been created since the previous records were released, in which case the updated data must be provided).
g. If the data that is requested is not the personal data of the requester, it cannot be released under an access request (unless it is the data of a child and is being requested by a legal guardian, or if it is data being requested by a solicitor with written consent from their client to access their data).

10. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Data Controller will promptly assess the risk to people's rights and freedoms. The Data Controller will also:

a. Give immediate consideration to informing those affected. Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the Data Controller may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.
b. In appropriate cases, the Data Controller will also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.
c. All incidents in which personal data has been put at risk will be reported to the Office of the Data Protection Commissioner as soon as the Data Controller becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or personal data of a financial nature.
d. When reporting to the Office of the Data Protection Commissioner in accordance with this policy, the Data Controller will make initial contact with the Office within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will not involve the communication of personal data. The need for a detailed report and/or subsequent investigation (based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data) will be determined by the Office of the Data Protection Commissioner.
e. Should the Office of the Data Protection Commissioner request a detailed written report of the incident, the report will reflect careful consideration of the following elements:

- a chronology of the events leading up to the loss of control of the personal data;
- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and / or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident; and
- the measures being taken to prevent repetition of the incident.

f. Even where there is no notification of the Office of the Data Protection Commissioner, the Data Controller will keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record will include a brief description of the nature of the incident and an explanation of why the Data Controller did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records would be provided to the Office of the Data Protection Commissioner upon request.

END OF POLICY