An Chomhairle Oidhreachta
The Heritage Council

General Data Protection Regulation (GDPR)

Code of Practice and Procedural Handbook

11th November 2021
Revised and updated

Table of Contents

1 Corporate GDPR Statement

The Heritage Council will, through its actions and policies, demonstrate that it cares for the personal data of people it interacts transparently, accountably, securely and in their interest in the first instance, and in the public interest thereafter, and that it will manage and monitor on an on-going basis its responsibilities as a 'data controller' in relation to the GDPR.

The Heritage Council undertakes to process all personal data with care for its ownership and integrity, and in accordance with the principles of GDPR. It will ensure that appropriate security measures are in place to protect confidentiality, and will review these from time to time with due regard to the technology available, the cost and the risk of unauthorised access.

This Code of Practice supports the provision of a management structure to assist the Heritage Council to comply with its obligations under GDPR, including the application of best practice guidelines and procedures in relation to all aspects of data protection. It shall be reviewed and updated in accordance with any legislative changes or other relevant indicators.

This Code of Practice and Handbook is to be read in conjunction with Council Staff Handbook, User Access Management Policy, Remote Access Policy, Security Awareness Policy, Mobile Devices Policy, Email Security Policy, Internet Security Policy, Anti-Virus/Malware Policy, and Anti-Fraud Policy. These associated documents contain important corroborative guidance as to how Council discharges its Data Protection duties.

2 What is GDPR?

The General Data Protection Regulation (GDPR) replaces and deepens the data protection laws that existed in the European Union pre-25th May 2018.

Its purpose is to safeguard the privacy rights of individuals in relation to the 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 of their personal data[1].

Data protection relates to you in two important ways:

- As a **data controller** Council holds, uses and processes personal data (about living persons) as part of its job.
- As a **data subject** where Council as an employer holds, uses and processes the personal data of its members staff and associates.

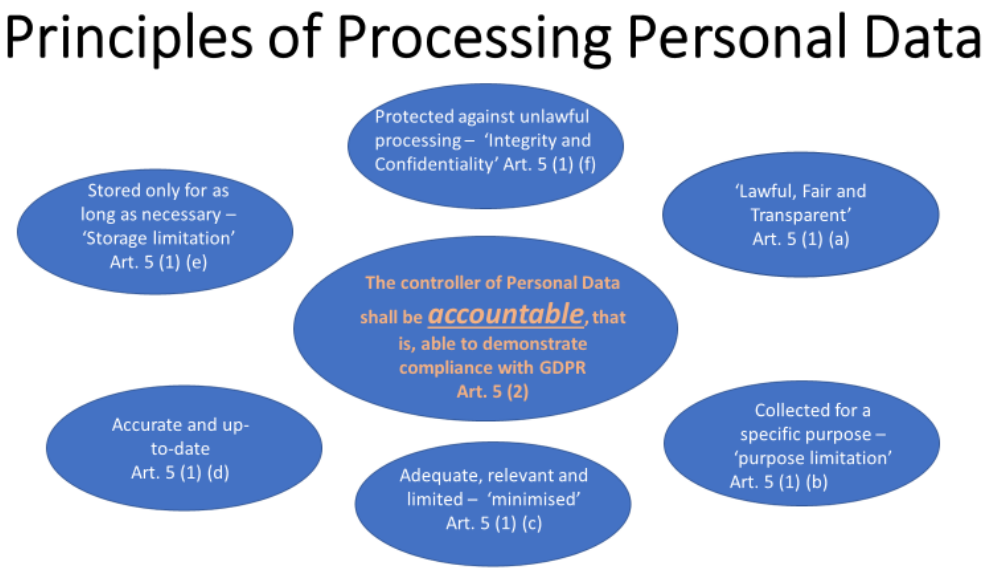
3 What is Personal Data?

Personal data means information relating to a **living individual** who is, or can be, **identified** either from the data or from the data in conjunction with other information that is in, or is likely to come into, your possession.

The definition of personal data is both technology neutral and format neutral. It includes data stored on a hosted or cloud service, computer network, hard drive, USB stick, internet, phone system, mobile devices (smartphone or tablet), camera, SD card, hardcopy paper file, electronic file, CCTV system, voice recording, etc.

1 Art. 4 (2), GDPR

The definition of personal data is deliberately broad. Examples of personal data include your name, address, phone number, email address, date of birth, bank details, signature, PPSN, photograph, video footage, employment records, salary records, medical records, your computer's IP address, voicemail, biometric data, etc.



The diagram summarises the six principles for 'processing' personal data defined in the GDPR, centring on Council's legal duty to demonstrate compliance. These principles should inform all actions of Council, its members and staff in their dealings with personal data.

4 What are the Implications of GDPR for the Heritage Council?

Data Protection relates exclusively to personal data held on a living individual who is, or can be, identified from that data.

In the context of the Heritage Council's work, the following areas broadly represent the greatest risk in terms of protecting personal data:

- **Children's data:** Publishing data on children, particularly in the context of social media.
- **Personal data published online:** Posting and sharing photographs and videos featuring identifiable people via social media and our websites (Heritage Week, Heritage in Schools and Heritage Council).
- **Personal data published in reports:** Publishing photographs featuring identifiable people in Heritage Council reports and publications.
- **Grants awarded to individuals**: Processing, storing and disclosing personal data relating to grants awarded to individuals.
- **Databases used for mailing list purposes:** Any databases containing personal data held by third parties on behalf of the Heritage Council for marketing, distribution and other purposes.
- **Contractual records:** Managing and storing internally sensitive contractual records of consultants engaged by the Heritage Council.
- **HR records:** Managing and storing employee HR records.

The key to GDPR compliance involves ensuring that personal data held on individuals is:

- Gathered only in relation to its statutory purposes, or with the consent of the data subject
- Published or disclosed only when consent is obtained
- Kept up-to-date and accurate

- Retained only for as long as is absolutely necessary
- If stored in Council's archives, then only for purposes related to heritage objects, and only for the purposes of identifying those objects
- Not used for any purpose other than that consented to by the individual.

5 The Heritage Council's Responsibilities as a Data Controller

The Heritage Council collects, controls and processes personal data tailored to its purposes, as set out in the following:

a) The public interest

b) Networking in the Heritage sector

c) Grant Schemes, consent basis

d) Board, staff, committee members

e) Potential conflicts of interest in decision-making

f) Contracts

g) Beneficial interest in Land

h) Interest in heritage

(a) The public interest

The statutory functions of the Heritage Council are set out in S. 6 of the Heritage Acts 1995 and 2018:

'The functions of the Council shall be to propose policies and priorities for the identification, protection, preservation and enhancement of the national heritage, including monuments, archaeological objects, heritage objects, architectural heritage, flora, fauna, wildlife habitats, landscapes, seascapes, wrecks, geology, heritage gardens and parks and inland waterways.' (S. 6 (1))

This description of the function of The Heritage Council outlines its public interest purpose. The definition of 'heritage object' includes *'objects over 25 years old which are works of art or of industry (including books, documents and other records, including genealogical records) of cultural importance'* (S. 2). The Heritage Council interprets this section to include archives and collections. The stewardship of archives for their material heritage interest, and for the information that they contain, which permits a greater understanding and deeper evaluation of other heritages, is promoted by the Council.

Council has processed data to make an archive of its previous surveying and grant-giving activity, which, by the nature of the records it made, may contain personal data in the form of names, addresses and contact details. It considers this to be compatible with S. 61(1) of the 2018 Act – 'processing of data for archiving purposes in the public interest'.

Council may address in the future the question of how to document intangible heritage, skills and practices that are possessed by people and which permit the transmission of cultural information, and which is intrinsically personal data.

The following particular clauses of the Acts require, permit or authorise the Council to obtain and process personal data.

(b) Networking in the Heritage sector, information provided in the course of communication

'The Council shall in particular

(a) promote interest, education, knowledge and pride in, and facilitate the appreciation and enjoyment of the national heritage,

(b) co-operate with, engage with, advise and support public authorities, local communities and persons in relation to the functions of the Council, and,

(c) promote the coordination of all activities relating to the functions of the Council.' (S. 3).

The Heritage Council thus engages in networking with individuals and persons in organisations who have interests in heritage. In this regard, its staff collect contact details of persons (business cards, addresses, phone numbers and email addresses from signature lines/ email footers, but not 'cc' lines) in the course of its business. Such information collected to develop a 'Heritage Sector' in Ireland by fostering interconnections and shares contact details.

(c) Grant Schemes, consent basis

'The Council may co-operate with and provide assistance and advice to any person or body, including a public authority, in respect of any matter which is related to the performance of its functions as it considers desirable.' (S. 11 (1))

The Heritage Council thus runs grant schemes, which require it to process grant applications from individuals, non-governmental organisations and other organs of the state, which include contact data, and the PPS numbers of individual people to comply with Tax Clearance Certificate requirements. This data is collected on the basis of consent, which must be freely given through the application process and which may be withdrawn.

(d) Board, staff, committee members, statutory basis

'The chairperson and members of the Council or of a committee of the Council shall be paid, out of monies at the disposal of the Council, such allowances for expenses incurred by them as the Minister, with the consent of the Minister for Finance, may determine.' (S. 14)

'The Council shall employ its own staff (an adequate number of whom should be competent in the Irish language so as to provide service through Irish as well as English) subject to such terms and conditions, including those relating to remuneration and superannuation, as it may, with the consent of the Minister and the Minister for Finance, determine.' (S. 18 (1))

'As soon as may be after its establishment the Council shall prepare and submit to the Minister a scheme or schemes for the granting of superannuation benefits on retirement or death to or in respect of such persons of its staff as the Council shall think fit.' (S. 20 (1))

The Council employs staff, about whom it will maintain employment, superannuation and human resources records. It holds personal data in relation to its employees to the extent appropriate for the management of the contract of employment and working relations.

The Council has a board with a chairman and can appoint committees to progress its work.

Council will use the names, and agreed descriptive personal profiles including photographs, of its employees and board and committee members in the course of its business, but will not release their contact details unless by specific prior agreement. Contact numbers of phones and e-mail addresses provided by Council to employees for work purposes will be made publicly available as appropriate.

(e) Potential conflicts of interest in decision-making, statutory basis

'Any member of the Council, or of a committee of the Council, who has a pecuniary or other beneficial interest in, or material to, any matter which falls to be considered by the Council or a committee of the Council, shall

(a) disclose to the Council or committee, as the case may be, the nature of that interest in advance of any consideration of the matter,

(b) not influence or seek to influence a decision in relation to the matter,

(c) take no part in any consideration of the matter,

(d) withdraw from the meeting at which the matter is being discussed or considered for so long as it is being discussed or considered by the Council or committee and shall not vote or otherwise act as such member in relation to the matter.' (S. 17 (1))

'A disclosure under this section shall be recorded in the minutes of the Council.' (S. 17 (4))

Members of the Board, and of committees set up by Council, should disclose pecuniary or other beneficial interests, which will be recorded in the minutes of meetings. Insofar as this amounts to personal data, it is likely to either require the minute of meetings to be held as a non-public record, or the record to have this material redacted if it is necessary or desirable to make it public.

(f) Contracts, statutory basis

'The Council may employ consultants or advisers on contracts for services as it considers necessary for the proper discharge of its functions.' (S. 18 (3))

'The Council shall keep, in such form as may be approved of by the Minister with the concurrence of the Minister for Finance, all proper and usual accounts of all monies received or expended by the Council, including an income and expenditure account and balance sheet and, in particular, shall keep all such special accounts as the Minister may from time to time direct.' (S. 21 (1))

The Council engages in contracts for service and supply in the course of its functions, and keeps accounts and financial records in relation to these, which include personal data. See also Section 18 below.

(g) Register of beneficial interest in land, statutory basis

'It shall be the duty of a person to whom this section applies ['… an employee of the Council or any other person whose services are availed of by the Council and who is of a class, description or grade prescribed for the purposes of this section' (s. 19 (2) (a)] *to give to the Council a declaration in the prescribed form, signed by that person and containing particulars of every interest which is an interest in* ['(i) any estate or interest which a person to whom this section applies has in any land, (ii) any business of dealing in or developing land in which that person is engaged or employed and any such business carried on by a company or other body of which that person (or a nominee) is a member, (iii) any profession, business or occupation in which such a person is engaged and which relates to dealing in or developing land' (S. 19 (2) (b)]*'* (S. 19 (1))

'*The Council shall, for the purposes of this section, keep a register (which register is in this section referred to as the register of interests) and shall enter therein the particulars contained in declarations given to the Council pursuant to this section.*' (S. 19 (7))

'The register of interests shall be available for inspection by the Minister.' (S. 19 (8))

The Council must maintain a register of interest in land, property development or business interests in the development of land and make the register available to the Minister at their request.

(h) Interest in heritage, statutory basis

'Each member of the Council shall be a person who, in the opinion of the Minister, has an interest in or knowledge or experience of or in relation to the national heritage.' (S. 5 Schedule, Art. 2 (2))

Council may need to specify the interest that the members of its board have in the national heritage, though experience to date indicates that everyone it encounters in its dealings has an interest to some greater or lesser degree in the national heritage.

As a data controller, there are 8 rules that must be followed. Council, its staff and members must:

- **Obtain and process information fairly.** At the time when you collect information on individuals, they must be made aware of how you are going to use that information. If you intend using this data for secondary purposes, they must be informed of these purposes and explicitly consent to this use of their personal data.

- **Keep it for a specified, explicit and lawful purpose.** You must be clear about the purpose for which you are keeping personal information on living individuals. It must be a lawful purpose e.g. legally or contractually necessary or necessary for the performance of a public body's function.

- **Use and disclose it only in ways compatible with this purpose.** Any use or disclosure must be necessary for and compatible with the purpose for which you collect and keep the data. You should ask yourself whether the data subject would be surprised to learn that a particular use or disclosure of their data is taking place.

- **Keep it safe and secure.** Adequate security provisions must be in place to protect personal data.

- **Keep it accurate, complete and up-to-date.** Data must be checked to ensure it is accurate and contemporaneous i.e. it must be updated over time.

- **Ensure that it is adequate, relevant and not excessive.** Where we collect personal data, it must be relevant and not excessive. In other words, if you were asked to justify every piece of information you hold on a given individual, could you do so?

- **Retain it for no longer than is necessary.** Personal data must only be kept for as long as it is needed for the purpose for which it was collected.

- **Make it accessible to that individual, and only that individual, on request.** Individuals should be informed of their right to get a copy of all personal data held on them.

6 Your Rights as a Data Subject

As a data subject, you have the following rights:

- **Right to have your personal data used in accordance with GDPR**. Your personal information must be obtained and used fairly, kept securely and only for as long as is absolutely necessary, and not illegitimately disclosed to others.

- **Right to be informed** about the type and extent of personal data collected or obtained from you and held by commercial companies and other organisations.

- **Right of access to your personal data**. You are entitled to get a copy of your personal information.

- **Right to rectification**. You have the right to have your personal information corrected where it is inaccurate or completed where it is incomplete.

- **Right to be forgotten**. You have the right to have your personal data erased if it is being unlawfully processed, held for longer than necessary, or used for direct marketing purposes.

- **Right to data portability** allows data subjects to get back personal data they provided to a company in a structured, commonly-used and machine-readable format and transmit that data to another company of their choosing e.g. emails held by an email service provider or data held by a music streaming service.

- **Right to object to processing** of your personal data, particularly where it relates to direct marketing or profiling.

- **Right to restrict processing** of your personal data. Where processing of your data is restricted, it can be stored by the data controller, but most other processing actions - for example deletion - will require your permission. A typical example is where you have contested the accuracy of your data and request a restriction until the data controller has determined the accuracy of your data, or the outcome of your objection.

- **Right to freedom from automated decision-making.** You have the right not to be subject to a decision based solely on automated processing e.g. creditworthiness, work performance, etc.

7 Making a Data Access Request

Data subjects are entitled to request copies of any personal details held on them by the Heritage Council, free of charge. The Heritage Council will provide this information within one month from date of receipt of the request, or sooner if possible. Council will use reasonable means to verify the requester's identity as the relevant data subject.

Where the data subject makes a request via email, the information will be provided in electronic format and sent to that email address, unless otherwise agreed. Where the data subject makes a request via post, the information will be provided in hardcopy format to the address provided, unless otherwise agreed. Information may also be provided orally, with careful consideration that the identity is of the data subject is verified.

Data subjects must submit a request in writing stating the exact information required.

Requests by email should be sent to: **dataprotection@heritagecouncil.ie**

Requests by post should be sent to: **The Data Protection Officer, The Heritage Council, Church Lane, Kilkenny, R95 X264.**

The data subject is only entitled to information that relates to them and will not be provided with data relating to other people or third parties.

Employees who record opinions about other employees in the course of their employment should bear in mind that these opinions may be disclosed to the data subject under an access request.

Please Note: The Heritage Council promotes an open access policy when dealing with data requests. Where possible, data requests shall be dealt with informally, outside of formal GDPR procedures.

8 Timeframes for Dealing with Data Requests

- Without delay and at the latest, within 30 days of receipt of the request.

- One month period may be extended by two additional months where necessary, with regard to the complexity and number of requests. The Heritage Council must inform the requester of any extension within one month of receipt of the request and the reasons for the delay.

- If the Heritage Council does not take action on foot of a data request, it must inform the requester without delay and, at the latest, within one month of receipt of the data request, of: (1) The reasons for not taking action (2) The possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Where Council has responded to a Data Subject Access Request, a record of that response (including (a) the electronic file compiled in processing the request and (b) the paper record of the data as issued) will be retained by Council until it receives a request from the Data Subject to delete it.

9 Making a Complaint

Under Article 77 of the GDPR, a data subject has the right to lodge a complaint with the Data Protection Commission if you consider that your personal data is being processed contrary to your rights under GDPR.

Under Article 78 of the GDPR, a data subject has the right to an effective judicial remedy where the Data Protection Commission does not handle your complaint or does not inform you, within three months, on the progress or outcome of your complaint.

Under Article 80, you may authorise certain third parties to make a complaint on your behalf.

Complaints to the Commission should be submitted in writing and addressed to:

info@dataprotection.ie

or

The Data Protection Commission, Canal House, Station Road, Portarlington, Co. Laois.

The Data Protection Commission also operates a **helpdesk** function, which is contactable at: **0761 104 800** or **LoCall 1890 252231**.

10 Data Protection Officer (DPO)

The Heritage Council's DPO reports directly to the CEO and Heritage Council board and is responsible for advising on and monitoring compliance with GDPR.

The role and duties of the DPO will be as set out in the Article 29 Data Protection Working Party's 'Guidelines on Data Protection Officers ('DPOs')'[2]. The DPO is completely independent and cannot receive any instructions regarding the exercise of duties from the board of the Heritage Council or its senior management team.

Council will put in place criteria for filling the role of Data Protection Officer to avoid potential conflicts of interest, and procedures for identifying future role-holders.

Council will identify a data protection team to fulfil its responsibilities to data subjects and the Data Protection commissioner.

[2] 'Guidelines on Data Protection Officers ('DPOs')', 2017, Article 29 Data Protection Working Party, Revised and Adopted on 5 April 2017, downloaded from http://ec.europa.eu/justice/data-protection/index_en.htm

11 Responsibilities of Staff, Contractors and Board Members

Employees, contractors and board members working for and on behalf of the Heritage Council are responsible for adhering to all GDPR policies and guidelines contained in this Code of Practice.

If an employee, contractor or board member is in doubt regarding their obligations, they should contact the Data Protection Officer for clarification.

Any breach of data protection policy is a serious matter and may lead to disciplinary action, up to and including dismissal.

Board members declaration of interest forms should only be accessible to authorised staff.

12 Project Planning and GDPR

The potential impact that a project or initiative might have on the privacy of individuals should always be considered. 'Data Protection Impact Assessment' (DPIA) will be integral part of all new projects i.e. data protection by design and not default. This will allow Council to identify potential privacy issues before they arise and come up with ways to mitigate them.

13 Photographs and Videos Featuring People

You need a person's consent (or parental consent for those under 18) when they are clearly recognisable in an image or video that you wish to share with a third party, post online or include in a hardcopy publication.

This is particularly important in the following circumstances:

- When dealing with children and minors under 18 years of age.
- Where circulation has a very wide reach and the potential for unauthorised reuse. Social media is a good example of this.
- Where a person or persons are the focus of an image or video e.g. posed photographs.

Consent can take the form of a simple announcement that you are about to take a photograph or video and giving people the option to step aside if they do not want to be included. However, there are certain circumstances when written consent will be required.

Photographing and filming large groups at a public event

If you are photographing or filming at a public event attended by large crowds, this is regarded as a public area so you do not need to get the permission of everyone in a crowd shot. People in the foreground of a crowd shot are also considered to be in a public area but you need to inform them of the fact and give them the option to step out of the photograph/video.

Photographing and filming individuals or small groups

Written consent should always be obtained from people whose images are the focus of the photograph or video. This also applies where a video or photograph incidentally captures passers-by in the background who are clearly identifiable.

To ensure compliance with GDPR:

- Ensure all those involved are aware/happy to be photographed or filmed.
- Obtain written permission from everyone involved.
- Obtain written permission from the parent/guardian of children or minors under 18 years of age. See Appendix A for consent form template.
- Signed consent forms must be retained and given to the Data Protection Officer.

Photographing and filming at a conference/seminar/event

To ensure compliance with GDPR:

- At the booking stage, inform them that photography/filming will be taken for social media and/or other purposes.
- At sign-in, include tick box to obtain consent for photography/filming.
- Always display a warning notice alerting delegates/attendees that photography or filming is going to take place
- Always verbally announce to those present that you will be photographing or filming, before starting to do so, so that those who have opted out may leave or move to the back of the room.
- Always offer those present the opportunity to sit somewhere they will not be photographed or filmed.
- Always inform those present of the purpose and use(s) to which images and recordings will be put.
- When children or minors are present at an event, it's highly recommended to use brightly coloured stickers to identify those who have not consented and ensure they are not inadvertently photographed or filmed.
- Signed consent forms are an extremely important record and must be retained and given to the Data Protection Officer.

14 Online Grants System - Awards to Individuals

Council has a standard operating procedure for the assessment of grants, which outlines the roles and responsibilities of those processing and assessing information in applications, including the confidentiality of personal data.

Financial data held on grant funded individuals (including invoices, PPSN, VAT numbers, bank account details, tax clearance access details, etc.) is held on a structured query database and is retained indefinitely in line with Council's statutory duties.

All data is hosted by a contracting processor on a secure encrypted server and appropriate contractual and security measures are in place to protect confidentiality. Technical support for Council's computers, cloud storage and email system is encrypted and stored in Irish data centres, and appropriate contractual and security measures are in place.

Feedback and data access requests in relation to unsuccessful applicants should be dealt with on an informal basis where possible i.e. outside formal data protection procedures.

Staff who deal with the administration of grants have an individual and collective responsibility to ensure that personal data relating to individuals is kept confidential and up-to-date.

Council's financial transactions are auditable by processes of internal audit, annual external audit and by the Comptroller and Auditor General. Invoices, including those that contain personal data, will be subject to processing by auditors in the course of Council discharging its fiduciary responsibilities.

15 Disclosure of Grant Recipient Data

The disclosure of grant recipient data by the Heritage Council is deemed to be in the public interest due to the fact that it is a public body administering public funds. Therefore, the Heritage Council has a corresponding duty to act in an accountable and transparent manner. This position is considered to be in full compliance with GDPR.

It is the policy of the Heritage Council to publish details of the projects it funds, including funding awarded to applicants who applied as individuals, in its Annual Report and financial statements. Typical data includes project title, location, amount awarded and recipient, who may be an individual.

From January 2017, applicants have been made aware of this policy when they apply for grants and it is highlighted on the application and declaration pages of the online grants system as follows: *'The Heritage Council publishes details of the projects it funds including project title, location and amount awarded. However, we do not publish the names of individuals and take all reasonable efforts to ensure that individuals are not identifiable from this data. Any personal information you give us will be processed, stored and managed in strict accordance with data protection legislation.'*

When retrieving and further processing information from its archive about places, it will replace location-defining information that is personal data with the relevant Eircode.

16 Heritage in Schools Programme

Financial data held on individuals providing services under the Heritage in Schools programme will be reviewed for destruction every 3 years due to the fact that these are ongoing relationships.

All data is hosted on a secure encrypted server and appropriate security measures are in place to protect confidentiality.

Feedback and data access requests in relation to unsuccessful applicants should be dealt with on an informal basis where possible i.e. outside formal data protection procedures.

Staff who deal with the administration of grants have a collective responsibility to ensure that personal data relating to individuals is kept up-to-date.

See under Section 19 for Garda vetting records.

17 Heritage Awards

The identity of an individual who makes a nomination under a Heritage Council awards scheme cannot be published or released without their written consent.

18 Personal Public Service Numbers

The Heritage Council is required to collect personal public services numbers (PPSNs) under Statutory Instrument 273 of 2011, Section 7.

PPSNs are collected and held on our financial management system and online grants system. Our financial management system is stored in-house on our secure server and is only accessible to authorised staff. Data stored on our online grants system is held on a database in a secure encrypted cloud space, hosted by a third-party service provider. See Section 14 above.

PPSNs collected by the Heritage Council are shared with the Office of the Revenue Commissioners only.

19 Garda Vetting Records

Garda vetting records are highly confidential and are securely stored in two locations. Access is strictly limited to the designated registered member of staff.

Garda vetting records are deleted one year after they are received, except in exceptional circumstances. In case of future queries or issues in relation to a vetting certificate the reference number and date of certificate are to be retained on file as this can be checked with An Garda Síochána.

20 Personal Data Held by Third Parties

Where personal data, collected by the Heritage Council, is hosted, processed or held by third party service providers, GDPR compliance requirements must be included in all contracts with the party hosting, processing or holding the data.

All contracts must explicitly state:

- The nature, purpose and duration of hosting, processing or holding personal data.
- The type of personal data and categories of data subjects.
- Personal data cannot be used, reused, disclosed, or shared with another party for any purpose(s) other than those specifically agreed upon and referred to in the contract.
- Personal data must be stored securely in accordance with European best practice operating and certification standards, and not US equivalents, in accordance with Article 32 of the GDPR. The location of the data must be clearly identified.
- Personal data must be retained only as long as is absolutely necessary to perform the specified contractual service. It is the responsibility of the service provider to ensure that data (including copies) is permanently and securely deleted once it is no longer needed.
- Third parties who engage in marketing/mailing services on behalf of the Heritage Council must ensure that all recipients (current and new) have '*actively'* consented to receiving these communications. Where de-registration is requested, the data subject's details must be removed immediately from mailing lists and the data subject must be informed that this has actually occurred. Every communication must include a consent 'opt out' facility.

The Heritage Council also processes data jointly with other parties, including the Department of Culture, Heritage and the Gaeltacht and the Department of Agriculture, Food and the Marine. Council will enter 'joint controller' arrangements with these organisations to give effect to the GDPR.

21 Sharing Contact Details of Individuals with Third Parties

If in doubt as to whether it is legally permissible to share an individual's contact details with a third party, please refer to the grounds on which Council collects data outlined at section 8 above. For further clarification, seek advice from the DPO.

Mailing lists and contact details
As a general rule, Heritage Council mailing lists and contact details of individuals should not be given by staff to third parties without the consent of the individual involved. However, discretion and common sense should be applied when making decisions in this regard.

Publication requests via courier
A contact phone number is required by the Heritage Council's courier service in order to process publication delivery requests. It is important to inform those requesting publications of the reason why this data is required.

22 Email Usage

Where an email is sent from the Heritage Council to multiple recipients outside the organisation, it should typically be done using the BCC (Blind Carbon Copy) field. This is particularly important when sending an email to recipients' personal email addresses, as opposed to a work email address.

As a general rule, email addresses obtained by Heritage Council employees from another source (e.g. email cc lists) should never be used or recycled for secondary purposes, without the consent of the addressee. The practice of gathering or collecting lists of email addresses without the consent of the individuals involved is known as email harvesting or spamming and is illegal. However, discretion and common sense should be applied when making decisions in this regard.

23 Mobile Device usage

Council has adopted a policy and code of practice for the use of mobile devices (mobile phones, tablets, etc) to address information security and health and safety in the use of these devices. This provides a framework for the protection of personal data collected in the course of work, held on these devices.

24 Social media usage

Council has adopted a policy and code of practice for (a) user's access to Council's ICT equipment, (b) internet security (c) anti-malware, and (d) policies in its Staff Handbook to address information security and health and safety in the use of these devices. This provides a framework for the protection of personal data collected in the course of work.

25 Employee Recruitment Records

Access to personal information is to be strictly limited to the individual to whom it relates.

Where applicable, external members of selection panels are to return all records to the Heritage Council on completion of the appointments process. It is the responsibility of the Chair of the selection panel to ensure that this is done.

Feedback and provision of reasons for decisions to unsuccessful applicants should be dealt with informally, where possible.

Record Description	Retention Policy
Records of unsuccessful applicants (shortlisted and not-shortlisted) including those who are successful but do not accept offer or take up employment	Destroy 1 year from date of completion of appointments process
Interview board marking sheet and notes	Destroy 1 year from date of completion of appointments process
Unsolicited applications for employment/ contract work	Respond and destroy immediately

26 Personnel Records

Disclosure of information contained in employee personnel, leave, expenses and payroll records is to be strictly limited to the employee to whom the data relates, subject to the administrative and operational needs of the Heritage Council.

Sick leave data will be recorded in minimal form on Council's internal shared calendar for management purposes only, and used by colleagues only to organise their working time (meetings, consultations, etc). It is not to be disclosed to prospective employers without the prior written consent of the data subject.

Employee personnel and payroll records are stored under secure conditions. Paper files are held in locked fireproof cabinets and electronic data on secure HR and Finance drives.

Managers are responsible for ensuring that all PMDS records they hold are stored securely and can only be accessed by authorised staff.

HR, senior management and finance staff with access to personnel, leave, expenses, payroll and superannuation records shall treat all information held and received in a strictly confidential manner and shall not disclose it, except where necessary in the execution of their official duties and functions, or in accordance with law.

Employees are responsible for ensuring that they inform the HR Officer of any changes to their personal details e.g. change of address.

Record Description	Retention Policy
Job application, CV and recruitment records, contract of employment, job description, terms and conditions of employment, references, probation records, training, personal development, PMDS and performance appraisal, salary and payment records, leave, timesheets, expenses, medical, health and safety, resignation/termination/ retirement letter, etc.	Retain for duration of employment. On retirement or resignation, hold for a further 6 years but retain service records for pension purposes
Pension/retirement records	Retain until pensioner and dependent spouse are both deceased and dependent children are finished full time education + 3 years

Disciplinary records – unfounded allegations and complaints	Destroy immediately but make a note on file that complaint was made. Do not keep detailed documentation
Disciplinary records – minor	Retain for duration of employment + 6 years
Disciplinary records – major/final warning	Retain for duration of employment + 6 years
Disciplinary records – involving criminal activity	Retain permanently

27 Records of External Personnel

Contracts of external personnel must include a statement relating to GDPR compliance as part of the terms and conditions of engaging services.

Hard copies of procurement/consultant files that are internally sensitive are to be stored in a locked filing cabinet or room to ensure they are not accessible to unauthorised personnel.

Electronic versions of procurement/consultant records that are internally sensitive are not to be stored on the R drive. Instead they should be emailed to the HR manager for storage on the secure HR folder. If you wish to keep reference copies, they should be stored in an appropriately named folder in MS Outlook.

Supplier invoices are to be stored in locked cabinets.

CVs and recruitment records relating to interns, consultants and panels should be retained only for as long as absolutely necessary.

Record Description	Retention Policy
Procurement – tendering and selection records	Rejected tenders – award of contract + 6 years
	Accepted tenders – termination of contract + 6 years
Consultant contract management - legal contract, performance, tax clearance, invoices and payment, general management and administration, etc.	Termination of contract + 6 years
Panels – CVs and profiles of consultants and individuals	Review for retention every 2 years
Interns – recruitment related records, CV, payment records, performance, general management and administration, etc.	Conclusion of internship + 2 years

28 CCTV

The Heritage Council operates CCTV in order to aid and improve the security of buildings and facilities and for the security and protection of staff.

CCTV images will be retained for a maximum of 28 days, except where the image identifies an issue and is retained specifically in the context of an investigation of that issue.

Any person whose image has been recorded has a right to be given a copy of the information recorded. This will only apply if the recording is available i.e. the request is made within the retention period outlined above. All requests should be submitted to the Data Protection Officer.

29 Keeping Data Secure

The physical security of premises, secure network and ICT systems, and good work practices are key to data protection compliance.

Premises

Premises are to be kept secure at all times. Access and egress to and from the Bishop's Palace is strictly controlled by an access control and image recognition system. All visitors are issued with a visitor identification badge and must sign in at reception.

For procedures in relation to out of hours work, please refer to the Heritage Council's Safety Statement (Nov 2015), page11.

Disposal of confidential waste

Appropriate procedures are in place for the disposal of confidential waste. Blue waste paper bins are located at workstations for the disposal of confidential waste.

Small quantities of confidential waste are also shredded onsite using in-house shredding equipment and disposed of confidentially. Larger quantities are outsourced to a specialist service provider where physical destruction is supervised by a member of staff and a destruction certificate obtained.

Cyber security

The Heritage Council's servers are hosted and managed by a third-party service provider with ISO 27001 certification.

Council's Staff Handbook contains its code of practice for employees in relation to Confidentiality (Section 5.9), E-mail and internet use (5.7) and Telephones (5.8).

Council's ICT operating platform and hardware have been hardened and encrypted to 2021 good practice standards, and will be continuously reviewed and upgraded on a monthly and quarterly basis. Hardware and software 'Firewalls' are in place, to protect end-user devices and the overall network. Devices, databases and files are encrypted at rest and in transit, and Transport Layer Security protocols have been added to e-mail systems.

Council has put in place a suite of employee policies for Information and Communication Technology usage, and associated risk management processes to measure, manage and remediate cyber risks.

All computer systems are password protected. The ICT system is set to lock computers if they are not accessed or used upon expiration of a predefined period of time and a password is required to unlock them.

Work practices

Personal security passwords are never to be disclosed to other individuals (including other employees).

At the end of each working day, staff are required to log out of computer systems and file/lock away any records containing personal data.

Laptops and other portable devices should never be left unattended when working offsite.

Personal data should never be stored on the hard drive of a portable device. Office 365 is to be used on portable devices for the creation and storage of any documents containing personal data.

30 Auditing

The Heritage Council will conduct an examination and review of data protection policies, procedures and risks associated with the storage, handling and protection of personal data on an annual basis. The Data Protection Officer will carry out this audit.

31 Reporting Personal Data Breaches

All staff, contractors, board members and third parties processing or storing personal data on behalf of the Heritage Council are responsible for reporting personal data breaches under Article 33 of the GDPR directly and immediately to the Heritage Council's Data Protection Officer.

The Data Protection Officer, in conjunction with the CEO, is responsible for deciding whether the breach needs to be reported to the Office of the Data Protection Commission.

Both officers will assess whether the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected.

If a risk to the data subject(s) is likely, the Data Protection Officer reports the breach to the Officer of the Data Protection Commission without undue delay, and not later than 72 hours.

If the data breach notification is not made within the mandatory 72 hour period, the Data Protection Officer submits it, without undue further delay, along with a justification for the delay.

If it is not possible to provide all of the necessary information at the same time, the Data Protection Officer will provide the information in phases without undue further delay.

The following information needs to be provided to the Data Protection Commission:

A description of the nature of the breach.
The categories of personal data affected.
Approximate number of data subjects affected.
Approximate number of personal data records affected.
Name and contact details of the Data Protection Officer.
Consequences of the breach (that have occurred + are likely to occur)
Any measures taken to address the breach.
Any information relating to the data breach.

If the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, the Data Protection Officer notifies those/the data subjects affected immediately.

The notification to the data subject must describe the breach in clear and plain language, in addition to information outlined in the table above.

The Heritage Council takes subsequent measures to ensure that any risks to the rights and freedoms of the data subject are no longer likely to occur.

The Data Protection Officer is responsible for documenting any personal data breaches, incorporating the facts relating to the personal data breach, its effects and the remedial action(s) taken.

32 Record keeping, information retrieval, electronic file structure

The Heritage Council's electronic document storage evolved over time iteratively, and which is therefore indexed with variable precision. The Head of Business and the Data Protection Officer will index or 'map' the information that Council archives, which may include personal data resulting from old work practices, to ensure efficient retrieval in the context of corporate memory, duties to disclose personal data and the smooth running of business.

Paper archives of business records are held in-office and an off-site archive.

To the extent compatible with ITC security, an outline of this archive structure will be included here to facilitate DSARs.

Appendix A

Template Consent Form for Filming and Photography

An Chomhairle Oidhreachta
The Heritage Council

Consent Form for Filming and Photography

Photographer/Videographer Information
Name:
Photo/Shoot Title:
Location:
Date:
Photographed/Recorded Person's Information
Name:
Are you over 18?:

Terms and Conditions of Use

- I hereby consent to the unrestricted use by the Heritage Council and those acting with its permission to use any images of me captured in video footage and/or photographs created today in any media (whether now known or hereafter devised), throughout the world, and for any purpose (excluding defamation) which may include, among others, advertising, promotion and marketing. The Heritage Council may also delegate, subcontract or assign such consent to any third party without consideration.
- I waive any right to inspect or approve the finished footage, imagery, advertising copy, text, or other printed matter that may be used in conjunction therewith.
- My image(s) will be held in accordance with GDPR (General Data Protection Regulation).
- Images of me captured in video footage/photographs will be the copyright of the Heritage Council and any other intellectual property which arises in the recordings will also belong to the Heritage Council.

Photographed/Recorded Person's Signature: _____

Name of Parent/Guardian if Person is under 18 years of age: _____

Signature of Parent/Guardian if Person is under 18 years of age: _____

Appendix B

Template

Filming/ Photography Location Warning Notice

An Chomhairle Oidhreachta
The Heritage Council

Location Warning Notice
Filming/Photography Taking Place Here

Please be advised that filming and/or photography will be taking place here in this area between the hours of [insert hours] **on** [insert date]

If you do not wish to be appear in any images captured, please

[Avoid this area at these times] *

[Sit at the back of the room] *

[Tell us so we can take appropriate steps to ensure you are not included] **

The photographs/film will be used by the Heritage Council for [insert details]. **They may also be used by The Heritage Council for promotional and communication purposes e.g. social media, publications, Heritage Council website, etc.**

[Insert other purpose as applicable] **

* please choose the appropriate sentence and delete the others
** please delete/complete as appropriate

Appendix C

Personal Data Classification, Handling and Retention Rules

Personal Data Classification, Handling and Retention Rules

11th November 2021. For adoption by Council

Data Category	Data Description	Data Subject Impact Classification	Storage and Security Rules	Access and Disclosure Rules	Retention Instruction
Employee recruitment records	Unsuccessful applicants (shortlisted), including those who are successful but do not accept offer	High	Store in (a) locked units and (b) on secure HR drive	Access strictly limited to data subject, HR section, recruitment consultants and members of appointments panel	Retain for 1 year from date of completion of appointments process
	Unsuccessful applicants who are not shortlisted	High	Deleted and destroyed at time of decision	Not applicable	Respond and destroy immediately
	Interview board marking sheets	High	Store in (a) locked units and (b) on secure HR drive	Access strictly limited to data subject, HR section	Retain for 1 year from date of completion of appointments process
	Interview board notes	High	Paper, or secure HR drive	HR manager and members of appointments panels	Destroy within one week of completion of interview
	Unsolicited applications for employment/contract work	Low	Not applicable	Not applicable	Respond and destroy immediately
Employee personnel / service records	Job application, CV and recruitment records, contract of employment, job description, terms and conditions of employment, references, probation records, training, personal development, PMDS and performance appraisal, salary and payment records, leave, medical, health and safety, resignation/ termination/ retirement letter, etc.	High	A single file for each employee. Store in (a) locked units until all have been migrated to (b) secure HR drive	Access strictly limited to data subject, HR section and CEO.	Retain permanently (until pensioner and dependent spouse are both deceased and dependent children are finished full time education + 3 years)
	Timesheets, attendance book	Low	Logbook kept at entrance desk	Accessible to staff only (fire safety, colleague availability)	
	Travel and subsistence expenses records	Low	(a) Pre-March 2021 paper record stored in locked units. (b) Post March 2021 digital record stored on secure HR drive and (c) at a drive location also available to the finance department	Access strictly limited to data subject, HR section, finance officer and CEO. Finance administrator has access to expenses and timesheet records only	Retain for 11 years
	Disciplinary records – unfounded allegations and complaints	Very high	Store in paper form only in locked units on personnel file only	Access strictly limited to data subject, HR section and CEO	Destroy immediately but make a note on file that complaint was made. Do not keep detailed documentation

Personal Data Classification, Handling and Retention Rules

Data Category	Data Description	Data Subject Impact Classification	Storage and Security Rules	Access and Disclosure Rules	Retention Instruction
	Disciplinary records – minor	Very high	Store in paper form only in locked units on personnel file only	Access strictly limited to data subject, HR section and CEO	Retain for duration of employment + 6 years
	Disciplinary records – major/final warning	Very high	Store in paper form only in locked units on personnel file only	Access strictly limited to data subject, HR section and CEO	Retain for duration of employment + 6 years
	Disciplinary records – involving criminal activity	Very high	Store in paper form only in locked units on personnel file only	Access strictly limited to data subject, HR section and CEO	Retain permanently
Workforce management records	Disability survey	High	Store in (a) locked units and (b) on secure HR drive	Access strictly limited to data subject, HR section and CEO. Anonymised return made to parent Department	Retain latest version only, destroy when superseded
Workforce management records	Covid-19 'Pre-Return to Work' forms	High	Store in paper form only in locked units on personnel file only	Access strictly limited to data subject, HR section and CEO	Retain until employee returns to work and then destroy
Externally procured services – consultants and individuals	Procurement – tendering and selection records	Low	Store on shared computer server (drive) or in enclosed units.	Access strictly limited to data subject, HR manager and members of appointments panel	Rejected tenders – award of contract + 6 years. Accepted tenders – termination of contract + 6 years
	Consultant contract management - legal contract, performance, tax clearance, invoices and payment, general management and administration, etc.	Low	Store on network or in enclosed units.	Open access internally on needs basis. Data is not to be disclosed to third parties unless explicitly consented to by data subject, or required by statute	
	Internally sensitive consultant contract management - legal contract, performance, tax clearance, invoices and payment, general management and administration, etc.	High	Store in (a) locked units and (b) on secure HR drive	Access strictly limited to data subject, line manager, HR manager and CEO	Termination of contract + 6 years
	Panels – CVs and profiles of consultants and individuals generated for procurement and contract management purposes	Low	Store on network or in enclosed units.	Open access internally on needs basis. Records are not to be disclosed to third parties unless explicitly consented to by data subject	Review for destruction every 5 years
	Interns – recruitment related records, CV, payment records, performance, general management and administration, etc.	High	Store in (a) locked units and (b) on secure HR drive	Access strictly limited to data subject, line manager and/or HR manager	Conclusion of internship + 2 years

Personal Data Classification, Handling and Retention Rules

Data Category	Data Description	Data Subject Impact Classification	Storage and Security Rules	Access and Disclosure Rules	Retention Instruction
Online grants system	Financial information held on grant applicants and grantees who receive funding – includes invoices, PPSN, VAT number, bank account details, tax clearance access details.	High	Hosted by external cloud provider on encrypted server	Data disclosed / shared with' Internal and external panel of grant assessors, financial section and data subject. System password protected	Retain and review with intention of deleting after 11 years
	Applications of individuals who apply for funding but are unsuccessful	Low	Hosted by external cloud provider on encrypted server	Data exclusively disclosed/shared with service provider and data subject. System password protected	Automatically deleted from system 18 months from date of application
	Applications of individuals who complete, or partly complete, online application but fail to submit it	Low	Hosted by external cloud provider on encrypted server		Automatically deleted from system 6 months from date application started
Historical Buildings at Risk survey and grant allocation database	Contact details of correspondents who supplied information about buildings they owned, for statistical survey purposes. Also used to apply for funding	Low	Access database on R: drive	Internal use only	Retain as historical archive
Glas Traditional Farm Buildings Grant Scheme	Administrative information on applicants and grantees - includes Herd no. (not considered personal data), address, PPSN, VAT number, bank account details, tax clearance access details. Future Joint Controller Agreement with Department of Agriculture, Food and the Marine	High	Stored in workspace of Project Manager, and in archive. From 2021, applicant data hosted by external cloud provider on encrypted server. Some personal data is Jointly Controlled with the DoAFM for purposes of grant payments.	Address all communication to grant applicant. Data exclusively disclosed / shared with grant assessors, Department of Agriculture, Food and the Marine, and data subject.	Locational and contact details (names and phone numbers) will be retained. Other personal data will be redacted from archive record after 11 years.
Heritage in Schools Programme	Financial data held on individuals providing services as contractors	High	Hosted by external cloud provider on encrypted server	Data exclusively disclosed/shared with financial section, and service provider as data subject. Restricted access. System password protected.	Review for destruction every 11 years
	Garda vetting access details – Particulars of any criminal record relating to the person, and a statement of the specified information (if any) relating to the person, or a statement that there is no criminal record or specified information, in relation to the person	High	Securely stored in single location - locked unit	Access restricted to Data Subject, CEO, Head of Communications and Heritage in Schools Programme Manager	Destroy 1 year from date of receipt, except in exceptional circumstances. Please note – Destruction record to include reference number and date of certificate to be retained on file

Personal Data Classification, Handling and Retention Rules

Data Category	Data Description	Data Subject Impact Classification	Storage and Security Rules	Access and Disclosure Rules	Retention Instruction
Financial records of historical payees	PPSNs, bank account details and contact details (address, phone and e-mail)	High	Store on secure finance drive in financial management system Also held in online grants system (encrypted cloud service) Historical information also held in paper files in locked presses in HC offices, and in off-site archive	Access restricted to Finance Officer and data subject	Retain indefinitely – required under Statutory Instrument 273 of 2011, Section 7. Irrelevant fields will be redacted.
	Salary and payment records for employees	High	Store in locked units, secure finance drive and financial management system	Access strictly limited to data subject and Finance Officer	Retain indefinitely.
Corporate governance	Board members declaration of interest forms	Medium	Store in (a) locked units and (b) on secure CEO drive	Access strictly limited to Secretary to the Board, CEO and PA to CEO. Used as required by Standing Orders for internal declarations of interest, and corporate reporting.	Retain for 11 years
Buildings management	CCTV images	Low	Stored on CCTV system and backup tapes	Access strictly limited to CCTV administrator, the data subject, and members of An Gardaí Siochana (in the event of criminal investigation)	Retain for maximum of 28 days, except where an image identifies an issue and needs to be retained specifically in the context of an investigation of that issue
Heritage awards	Name and contact details of person making or submitting a nomination	Low	Word document (server), held by Head of Communications	Written consent to be obtained and given to DPO before sharing or publication occurs	Destroy once award is given. Retain other supporting information if necessary
Heritage Council Websites (e.g. www.heritagecouncil.ie, www.heritageweek.ie, and www.heritageinschools.ie)	Cookies. Only the anonymised internet service provider number of user is collected.	Low	Policy reviewed annually	Heritage Week website log-in details shared with HW contractor.	Retain for 1 year
GDPR compliance	Signed consent forms	Low	Held by DPO in locked unit. Store on network or in enclosed units. Do not store in open units or on workstation desks/floor	DPO access only	Retain for duration of employment + 6 years

Personal Data Classification, Handling and Retention Rules

Data Category	Data Description	Data Subject Impact Classification	Storage and Security Rules	Access and Disclosure Rules	Retention Instruction
	Personal data subject access (DSAR) requests	High	Held by (a) DPO locked unit and, if necessary, (b) on secure DPO drive	Access strictly limited to DPO section and CEO	Retain until file closed, destroy and create record of destruction
Freedom of Information (FoI) requests	Requests containing personal data	Low	Held by (a) FoI section locked unit and, if necessary, (b) on secure FoI drive	Access strictly limited to FoI section, and CEO	Retain until file closed + destroy
Photographs and videos featuring identifiable people	Minors (under 18 years of age)	High	Stored on network, cloud, personal hard drives, mobile devices (phones, laptops), hard copy. Heritage Council's purpose of taking photo or making video to be stated.	Signed consent forms to be obtained and given to DPO before sharing or publication occurs	Retain indefinitely – historical record
	Adults	Medium	Stored on network, personal hard drives, mobile devices (phones, laptops), hard copy. Heritage Council's purpose of taking photo or making video to be stated	Signed consent forms to be obtained and given to DPO before sharing or publication occurs	Retain indefinitely – historical record
Membership of external recruitment panels	Recruitment, selection, interview board and appointment records	Follow GDPR directive of relevant authority/body	Follow GDPR directive of relevant authority/body	Follow GDPR directive of relevant authority/body	Repatriate to relevant authority/body or destroy. These records are not to be held by the Heritage Council
Historical membership of external committees and boards	Where personal data historically was created, received or stored by the Heritage Council	Measured on case by case basis	Follow GDPR directive of relevant authority/body	Follow GDPR directive of relevant authority/body	Repatriate to relevant authority/body where applicable and destroy.
Mailing lists and contact details of individuals	Name, address, personal email address, landline number, mobile number, contact history/profile, etc.	Low	Data held on phones, email systems, mailing lists, spreadsheets, databases, notebooks, etc.	Data is not to be shared with third parties unless consent is explicitly obtained from data subject(s)	Review data for GDPR consent/data cleansing every 2 years