OPW
Oifig na nOibreacha Poiblí
The Office of Public Works

The Office of Public Works

Data Protection Policy

Jonathan Swift Street
Trim, Co Meath
Ireland, C15 NX36

www.opw.ie

V2.0

4 October 2018

Contents

1. Summary

Key definitions

Data Subject: A living person who can be identified; whose personal data is processed.

Personal Data: Any information relating to a data subject, e.g. name, PPSN, PMDS. Special categories of these reveal a person's political opinions or health.

Controller: The entity that determines the purposes and means of the processing.

Processor: The entity that processes on behalf of the controller, e.g. PeoplePoint.

Processing: **Any operation performed on personal data, e.g. storage or destruction.**

Supervisory Authority: The Irish Data Protection Commission is responsible for data protection .

Scope

This policy applies to all OPW staff, contractors and processors.

The Data Protection Principles

1. **Lawfulness, Fairness and Transparency**
   Data subjects must be told how their personal data will be used before it is processed. Lawful processing requires processing to have a legal basis, which also must be made available to data subjects. See **Our Procedures** below for details.

2. **Purpose Limitation**
   Data can only be used for specified, explicit and legitimate purposes.

3. **Data Minimisation**
   Any data collected must be necessary and not excessive for its purpose.

4. **Accurate**
   The data we hold must be accurate and kept up to date.

5. **Retention**
   We cannot store data longer than necessary.

6. **Integrity and Confidentiality**
   The data we hold must be kept safe and secure.

7. **Accountability**
   We must comply with all these principles and be able to prove that we comply.

8. **Data Subject Rights**
   We must allow data subjects to exercise their rights

Our Procedures for Fair, Transparent and Lawful Processing

We must process personal data **fairly, transparently and lawfully**. We must inform data subjects informed in advance of the purposes of the processing. Lawful processing requires that at least one of the following legal bases must apply:

a) Consent
The OPW cannot generally use consent as a public body or as an employer

b) Contract
The processing is necessary to fulfil or prepare a contract (e.g. procurement).

c) Legal Obligation
We have a legal obligation to process the data. We must cite the relevant statute.

d) Vital Interests
The processing is necessary to protect a person's vital interests (e.g. life or death).

e) Public Interest
The processing is necessary to carry out a task in the public interest or in the exercise of our official authority. We must cite the relevant statute.

f) Legitimate Interest
The processing is necessary for our legitimate interests. We cannot use this basis for our statutory or public interest functions.

If you are deciding which lawful basis to use, choose that which best fits the purpose, not what is easiest and have it approved by the DPO. You must document this process to show that you have considered which lawful basis best applies and can fully justify it. We must inform data subjects both of the lawful basis for processing their data and the intended purpose in a privacy statement. This applies whether we have collected the data directly from the individual, or from another source.

Responsibilities

1. Responsibilities of the OPW

- Analyse and document the type of personal data we hold
- Identify the lawful basis for processing data
- Detect, report and investigate personal data breaches
- Conduct Data Protection Impact Assessments for all new or high-risk processing.
- Store personal data safely and securely
- Assess the risks that processing could pose to individual data subjects

2. Your Responsibilities

- Undergo training and fully understand your data protection obligations
- Check your processing is lawful, justified and compliant with our policy

- Do not infringe data protection laws or our policies through your actions
- Immediately report any concerns, breaches or errors to the DPO
- **Never** disclose or allow anyone else to use your password and **never** write it down
- Always lock your screen whenever you leave your PC
- Check that you have the correct recipient(s) when sending emails
- Do not leave personal data lying around. Lock it away and keep the key out of sight.

3. Responsibilities of Those Engaged in Marketing, Promotion or Event Management

- Ensure that privacy statements attached to emails and other marketing/publicity material meet the requirements of GDPR
- Do not use "opt-out" consent. Ask for further consent with each follow-up email, as required. Only retain any personal data for marketing for at most 1 to 2 years.
- Direct data protection queries from clients or the media to the DPO for advice
- Coordinate with the DPO to ensure all marketing initiatives (e.g. email harvesting) adhere to data protection laws and the OPW's Data Protection Policy
- Ensure that when photographs or videos are to be taken at OPW-organised events where individuals may be identified, attendees are notified in advance that such photography may take place, are made aware of its purpose and are given an opportunity to object, if they wish

4. Accuracy and Relevance

Any personal data we process must be accurate, adequate, relevant and not excessive for the purpose for which it is processed. Individuals may ask that we correct their inaccurate personal data.

5. Data Security

You must keep personal data secure against loss or misuse. Where other organisations process personal data on our behalf, they must be contractually obliged to guarantee that they will implement appropriate security measures to protect it.

6. Storing Data Securely

Keep personal data stored on paper in a secure place. Printed data should be cross-cut shredded when it is no longer needed. Protect electronic data with strong, regularly changed passwords. Portable storage devices such as memory sticks must be encrypted or password protected and should be locked away when not in use. The DPO must approve any cloud-based service that is processing personal data. Servers containing personal data must be kept in a secure location and protected by security systems. Data should be regularly backed up. Mobile devices such as laptops or smart phones must be encrypted. Take all possible technical and organisational measures secure personal data.

7. Data Retention

We must not retain personal data for longer than is necessary. Data cannot be kept forever, or just in case it is needed – it must be necessary. All personal data items must have a retention period. This will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a line with our data retention guidelines. These will be determined when completing the online questionnaires and published in our Record of Processing Activities.

8. Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data outside the EEA or to an international organisation unless:

- ☐ It is to a country that the EU Commission has decided offer adequate levels of data protection (e.g. Switzerland). Contact the DPO for the current list.
- ☐ One of the following safeguards is in place:
  - Legally binding and enforceable instruments between public bodies
  - Binding corporate rules
  - Model contracts (with approved standard data protection clauses)

Using cloud-based or web-based systems could be transferring data abroad. Always insist on suppliers telling you where the data will be stored.

Data Subject Rights and How to Deal With Them

Data subjects have rights regarding their personal data and we must permit them to exercise their following rights:

1. Right to be Informed

We must provide intelligible privacy statements (aka privacy notices) explaining what personal data we are processing, what we are doing with it, the legal basis for the processing and what degree of privacy the data subject may expect. A privacy statement must be supplied at the time the data is obtained directly from the data subject, otherwise, within one month of obtaining the data. On forms and websites forms where space is limited, use the following text (approved by the AGs) including a link to the appropriate privacy statement:

> *The personal data that you provide to the OPW will be processed and shared in accordance with the law. See http://www.opw.ie/data_protection/<Your-OPW-privacy-statement.pdf>.*

A privacy statement must be concise and written in clear and plain language. The information that must be included in a privacy statement can be found in Section 11 of this policy. A template privacy statement is available on Stór.

2. Right of Access

In response to Data Subject Access Requests (DSARs), we must confirm to data subjects that we are processing their personal data and provide then with a copy of it. We must provide a data subject with the necessary information and a copy of their data, free of charge, within one month of validating their identity. We must supply the information in writing or electronically, where possible, matching how it was requested, or as requested. Where technically possible, if requested, information may be provided orally. Where the request is complex or numerous requests are made, the deadline can be extended by two months, but the data subject must be informed within one month.

3. Right to Rectification

We must rectify the personal data of a data subject on request if it is inaccurate.

4. Right to Erasure

We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing. We can only refuse to erase the data to comply with a legal obligation; to perform a task carried out in the public interest; to perform a task in the exercise of official authority or to archive personal data.

5. Right to Restrict Processing

In certain circumstances we must comply with requests to restrict our processing of personal data. We can only store restricted personal data, but cannot process it otherwise, unless the data subject consents; to establish, exercise or defend legal claims; to protect the rights of others or for important public interest reasons.

6. Notification Obligation

We must notify recipients of any rectification, erasure or restriction of personal data unless this proves impossible or involves disproportionate effort.

7. Right to Data Portability

Where the lawful basis of an automated processing activity is consent or a contract, we must provide data subjects with their personal data in a commonly used, machine-readable format so that they can reuse it for their own purposes or on different services or send it directly to another controller on request.

8. Right to Object

Where data subjects object to the processing of their personal data, we must cease the processing, unless we can demonstrate compelling legitimate grounds for the processing that override their interests, rights and freedoms; the processing relates to the establishment, exercise or defence of legal claims; the processing is for scientific or historical research in the public interest. If we are processing the data for direct marketing, we must then cease the processing. We must always explicitly inform the data subject of their right to object at the first point of communication with them and provide an automated way for data subjects to object in online services.

9. Rights in Relation to Automated Decision Making and Profiling

In certain circumstances, data subjects have the right not to be subjected to solely automated decision making and profiling which significantly or legally effects them.

Processors

As a controller, the OPW must have binding, written contracts place with processors that process personal data on our behalf. These contracts must set out the subject matter and duration of the processing, the nature and stated purpose of the processing, the types of personal data and categories of data subjects, and the obligations and rights of the controller. Details are in Section 14. We must only appoint processors who provide sufficient guarantees that their processing will comply with the GDPR and will protect the rights of data subjects. We may be legally liable for failures of our processors to comply with the GDPR.

Criminal Offences and Convictions

Data relating to criminal convictions and offences is a special category of personal data. It must be handled carefully due to its sensitivity and the risk it presents to its data subjects. The processing of such data must have a legal basis, safeguarding the fundamental rights and freedoms of the data subject and at least one of the lawful grounds below should apply:

- It is processed under the control of official authority for purposes such as the administration of justice; regulatory, authorisation or licensing functions; determining eligibility for benefits or services; regulating professions; enforcement or archiving in the public interest. As we are not involved in these activities, this is not a legal ground for vetting the staff of contractors or subcontractors
- The data subject has given explicit consent (to the National Vetting Bureau (NVB) - not to the OPW) for the vetting by signing the Garda vetting form.
- The processing is necessary and proportionate for the performance of a contract to which the **data subject is a party or** to take steps at the request of the **data subject** before entering into a contract. We can vet our own staff as we have a contract. We have contracts with our contractors, but not with their staff.
- The processing is permitted by law, as is the case for vetting for child protection.

We cannot force staff to apply for vetting themselves and to give us their vetting disclosure. Details of the vetting process and the data protection implications are in Section 15. Only OPW liaison persons may handle vetting. They are the sole point of contact with the NVB

Drones

Drones with cameras are subject to the OPW CCTV Systems Data Protection Policy. Drones must comply with the Irish Aviation Authority regulations on drone usage. Drones cannot be used at National Monument sites, near other aircraft, within 5km of an airfield, over 300m from the operator or higher than 120m. The OPW should never use drones for covert surveillance.

Before drones are used in an area, the flights should be publicised via signs, posters, leaflets, social and local media, so that people are adequately and clearly informed. Information on upcoming and past uses of drones should be published on the OPW website. Drones should be conspicuous, using bright colours, flashing lights or sirens and be OPW-branded. The drone operator should be clearly identifiable as the person responsible for the drone.

Drone video footage containing inadvertently captured personal data should be deleted or anonymised using software to blur faces or registration numbers. Any data captured should be stored in a secure environment. Access to the data should be controlled, logged and monitored. Footage should be encrypted and only made available only to authorised users.

Drone operators working on behalf of the OPW are processors and the rules in Section 14 also apply to them. The data subject rights in Section 12 of this document apply to those whose data is captured by a drone. The rules in Section 18 on data breaches also apply to drones. Where an Garda Síochána seek drone footage for a criminal investigation, the rules for CCTV footage set out in the OPW CCTV Systems Data Protection Policy apply.

Data Audits, Monitoring, Compliance and Training

The DPO will carry out regular data audits to identify risks and monitor compliance with this policy and data protection law. Everyone must observe this policy and the law. We take compliance with both very seriously. Failure to comply puts both you and the organisation at risk. Such failures are infringements, which must be reported to the DPO as soon as possible. Failure to comply may lead to disciplinary action. You will receive training on provisions of data protection law specific to your role. This training is mandatory. If you move role, you must request training for your new role.

Reporting Data Breaches

Any loss, theft or destruction of personal data by the OPW or its processors, accidental or otherwise, is a data breach, e.g. sending an email containing personal data to the wrong recipient, the loss or theft of unencrypted mobile device or a cyber-security incident, e.g. hacking, denial of service or data theft. It is **mandatory** for the OPW to report any data breaches to the Data Protection Commission (DPC) **within 72 hours of first becoming aware** of ithe data breach. All staff must I**mmediately** report any actual or suspected data breaches **to the DPO** (or one of his or her staff). All breaches must be documented bu t the DPO decides which must be reported to the DPC.

OPW Data Protection Registers

The OPW maintains four Data Protection registers:

- Registers of Processing Activities and of Personal Data Repositories
  These are maintained via online questionnaires and will be widely circulated to staff. These must be completed quickly and accurately, as the information they gather is legally required.
- Register of Personal Data Breaches
  This register records details of all actual or potential data breach incidents and is compiled by the DPO as staff report them.
- Register of Data Subject Access Requests **(DSARs)**
  As DSARs are received, the DPO compiles a register of those requesting them to determine if they are excessive or repetitive.

2. Introduction

The Office of Public Works (OPW) holds personal data about employees, clients, suppliers and other individuals for a variety of business purposes. The OPW is committed to protecting the rights and freedoms of data subjects and to safely and securely processing their data in accordance with all of our legal obligations under the EU General Data Protection Regulation (GDPR) - effective from 25 May 2018 and the Data Protection Acts 1988 to 2018.

This policy sets out how we seek to protect personal data and ensure that our staff, contractors, processors and those who use our systems understand the rules governing their use of the personal data to which they have access in the course of their work.

This policy requires staff and those who use our systems to consult the Data Protection Officer (DPO) before any significant new data processing activity is initiated, to ensure that relevant compliance steps are addressed.

This policy applies to **all processing activities within OPW relating to personal data** including processing performed by other bodies (processors) on OPW's behalf. It applies to processing of personal data, wholly or partly by:

- automated means (ICT systems).
- non-automated (manual) processing which forms, or is intended to form, part of a filing system.

3. Definitions

Purposes of Processing	A full list of purposes for which we process personal data can be found in the OPW's Register of Processing Activity on the OPW's website, but is too long to reproduce in this document. The **main purposes for which we process** personal data include the following: • Purchasing, selling, leasing, managing and maintaining accommodation for Government bodies • Undertaking design, development, construction, refurbishment and conservation projects for the State • Booking tours groups, selling heritage cards, direct marketing, guide recruitment and administration • Public consultation on flooding schemes and studies • Online mapping for flood hazards and erosion, drainage schemes, flood risk management plans, flood risk management and defended areas; real time hydrometric data and flood studies web portal • Administering Voluntary Home Relocation Scheme • Maintaining arterial drainage schemes and providing consent for bridges and culvert works • Personnel, administrative, financial, payroll and business development purpose • Developing, maintaining and securing ICT systems • Learning and development and continuous professional development • CCTV systems • Child protection vetting • Compliance and Data Protection auditing • Equality and workplaces Investigations • Health and safety monitoring • Procurement
Data Subject	A living person who can be identified, directly or indirectly, by an identifier such as a name, an ID number, location data, or by factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. In other words, a data subject is the person whose personal data is processed.

Personal Data	Any information relating to an identified or identifiable living person (*data subject*). An identifiable person can be identified, directly or indirectly, by an identifier such as a name, an identification number, location data or by factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity. The personal data we process may include individuals': names; PPSNs; home addresses; medical certificates and records; bank, revenue, financial and pay details; phone numbers; email addresses; photographic and video images; education and skills, details of degrees, certificates and diplomas, training records; marital status, nationality; email addresses; social media posts; travel claims; PMDS; CVs and application forms, interview notes; HR files; IP addresses.
Special Categories of Personal Data	Personal data revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, criminal offences or related proceedings, sex life or orientation and genetic and biometric information. Processing of such data is prohibited except in strictly controlled circumstances.
Controller	A person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In this policy, the controller is the Commissioners of Public Works in Ireland.
Processor	A person, public authority, agency or other body, which processes personal data on behalf of the controller. Examples include shared services such as PeoplePoint, Payroll Shared Services Centre, etc.
Processing	Any operation performed on 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. Note that collecting personal data but never using it is still is processing, as is destroying personal data.
Profiling	Automated processing using personal data to analyse or predict a data subject's work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
Supervisory Authority	This is a national or regional body responsible for data protection. The Irish supervisory authority is the Data Protection Commission.

4. Scope

This policy applies to:

- All staff, who must be familiar with this policy and comply with its terms.
- Contractors and others, who use OPW systems containing personal data
- Processors who process data on behalf of the OPW

This policy supplements our other policies relating to Internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated before being adopted.

Who is responsible for this policy?

The OPW Data Protection Officer (DPO) is responsible for the content of this policy and for keeping it up to date. All OPW staff, contractors and consultants who process personal data in the course of their work are responsible for the day-to-day implementation of this policy. You should contact the DPO for further information about this policy if necessary (dpo@opw.ie).

5. The Data Protection Principles

The Office of Public Works shall comply with the principles of data protection (the Principles) enumerated in the General Data Protection Regulation. We will make every effort possible in everything we do to comply with these principles.

The Principles are:

1. **Lawfulness, Fairness and Transparency**
   Personal data must be processed lawfully and fairly. We must be open and transparent with data subjects as to how the data will be used.

2. **Purpose Limitation**
   Data can only be used for specified, explicit and legitimate purposes. It cannot be used for any other purposes.

3. **Data Minimisation**
   Any data collected must be necessary and not excessive for its purpose.

4. **Accurate**
   The data we hold must be accurate and kept up to date.

5. **Retention**
   We cannot store data longer than necessary.

6. **Integrity and Confidentiality**
   The data we hold must be kept safe and secure.

7. **Accountability**
   See below.

8. **Data Subject Rights**
   We must allow data subjects to exercise their rights

Appendix 1 provides further information on Data Protection principles.

Accountability and Transparency

We must ensure accountability and transparency in all our use of personal data. It is not enough to say that we comply with the GDPR. We must be able to show how we comply.

You are responsible for keeping a written record of how all the data processing activities you are responsible for comply. This will be done via online questionnaires to be completed for every processing activity and data storage asset. The DPO will meet each business area to help identify their processing activities and assets. This record must be kept up to date and must be approved by the DPO.

To comply with data protection laws and the accountability and transparency Principle of GDPR, we must demonstrate compliance. You are responsible for understanding your particular responsibilities to ensure we meet the following data protection obligations:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities
- Conducting Data Protection Impact Assessments
- Implement measures to ensure privacy by design and default, including:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Creating and improving security and enhanced privacy procedures on an ongoing basis

6. Our Procedures

Fair and Lawful Processing

We must process personal data **fairly, transparently and lawfully**. This generally means that we should not process personal data unless the individual whose details we are processing **is informed in advance of the purposes of the processing**.

If we cannot apply a lawful basis (explained below), our processing will infringe the GDPR and be unlawful. Data subjects have the right to complain to the Data Protection Commission or seek legal redress against the OPW for such infringements.

If you are in any doubt about how we handle data, contact the DPO for clarification.

Lawful Basis for Processing Data

We must establish a lawful basis for processing data. Ensure that any personal data you are responsible for managing has a **written lawful basis approved by the DPO**. It is your responsibility to confirm the lawful basis for any processing of personal data . To be lawful, a**t least one** of the following conditions must apply whenever we process personal data:

1. **Consent**
   The OPW cannot generally use consent as a public body, because of the imbalance between the State and an individual. Equally, there is an imbalance between the OPW as an employer and an individual employee. We can use consent in limited circumstances but must hold recent, clear, freely given, explicit, and defined consent for the individual's data to be processed for a specific purpose.

2. **Contract**
   The processing is necessary to fulfil or prepare a contract for the individual (e.g. procurement).

3. **Legal Obligation**
   We have a legal obligation to process the data (excluding a contract). The statute imposing the obligation must be cited in the Record of Processing Activity and the Privacy Statement.

4. **Vital Interests**
   Processing the data is necessary to protect a person's vital interests (e.g.to protect life or health in an emergency a medical situation.

5. **Public Interest**
   Processing necessary to carry out a task undertaken in the public interest or in the exercise of our official authority. The statute on which this is based must be cited in the Record of Processing Activity and the Privacy Statement.

6. **Legitimate Interest**
   The processing is necessary for our legitimate interests. This ground is extremely very limited for the OPW and cannot be used for our statutory or public interest functions. You should not rely on this as a lawful ground.

Deciding Which Condition to Rely on

If you are making an assessment of the lawful basis, you must first establish that the processing is necessary. Remember that more than one basis may apply, and you should rely on what will best fit the purpose, not what is easiest.

Consider the following factors and document your answers:

- What is the purpose for processing the data?
- Can it reasonably be done in a different way?
- Is there a choice as to whether or not to process the data?
- Who does the processing benefit?
- After selecting the lawful basis, is this the same as the lawful basis the data subject would expect?
- What is the impact of the processing on the individual?
- Are you in a position of power over them?
- Are they a vulnerable person?
- Would they be likely to object to the processing?
- Are you able to stop the processing at any time on request, and have you factored in how to do this?

Our commitment to the first Principle requires us to document this process and show that we have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

We must also ensure that individuals whose data we process are informed of the lawful basis for processing their data, as well as the intended purpose. This should occur via a privacy statement. This applies whether we have collected the data directly from the individual, or from another source.

If you are responsible for making an assessment of the lawful basis and implementing the privacy notice for the processing activity, you must have this approved by the DPO.

7. Special Categories of Personal Data

What Are Special Categories of Personal Data?

Previously known as sensitive personal data, this is data about an individual which is more sensitive in nature, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example, by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- Race
- Ethnic origin
- Political opinions
- Religion
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sexual orientation

In most cases, the processing of special categories of personal data is prohibited, unless one of a number of conditions applies, such as:

- Data subject has given their explicit consent for the processing for specific purpose(s)
- Processing is necessary to protect the vital interests of the data subject
- The data subject has manifestly made the personal data public
- Processing is necessary to establish, exercise or defend legal claims

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data ,that processing activity must cease.

8. Closed Circuit Television (CCTV)

The management and use of Closed Circuit Television (CCTV) is covered in the related OPW CCTV Systems Data Protection Policy.

9. Responsibilities

Responsibilities of the OPW

- Analyse and document the type of personal data we hold
- Check procedures to ensure they cover all the rights of the individual
- Identify the lawful basis for processing data
- Conduct a Data Protection Impact Assessment (DPIA) for new or high-risk processing, e.g. the large scale, systematic monitoring of a public area. Seek the advice of the DPO as necessary. Note that the DPO does **not** undertake DPIAs
- Implement and review procedures to detect, report and investigate personal data breaches
- Store data in safe and secure ways
- Assess the risk that could be posed to individual rights and freedoms should data be compromised

Your Responsibilities

- Fully understand your data protection obligations
- Check that any data processing activities you are dealing with are lawful, justified and comply with our policies at all times
- Do not use data in any unlawful way
- Do not store data incorrectly, be careless with it or otherwise cause us to infringe data protection laws or our policies through your actions
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or our legal obligations to the DPO without delay
- Use passwords properly and securely
- Never allow other to use your user name or password. Never disclose your password to others (unless authorised to do so by the ICT Unit troubleshooting ICT problems).
- Never write your password in desk diaries or on Posts-Its stuck on screens or under computers.
- Always lock your screen whenever you leave your PC
- Be particularly careful that you have the correct recipient(s) in To, CC and BCC fields when sending emails containing personal data.
- Do not leave personal data lying around, either on your desk or on top of presses/filing cabinets. Lock it away and remove the key from the lock, storing it out of sight.

Responsibilities of the Data Protection Officer

- Keep the Management Board updated about data protection responsibilities, risks and issues
- Review all data protection procedures and policies on a regular basis
- Arrange data protection training and advice for all staff members and those included in this policy
- Answer questions on data protection from staff, managers, Management Board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know what data we hold on them
- Check and approve third parties that handle the company's data any contracts or agreement with processors that process personal data processing
- Assess, log and coordinate Data Subject Access Requests (see 12 below)
- Coordinate a response to data breaches involving personal data (see 18 below)

Responsibilities of the ICT Unit

- Ensure that all systems, services, software and equipment meet acceptable security standards
- Check and scan security hardware and software regularly to ensure it is functioning properly
- Review data repositories on an ongoing basis to ensure that personal data is secured and that activities associated with it are logged
- Take technical measures to protect personal data on OPW computers and mobile devices. This includes access control to systems, so that only authorised staff can view personal data
- Deploy data backup systems to ensure that personal data can be recovered if lost, deleted, destroyed or corrupted, through techniques such as backup and recovery, replication and disaster recovery plans
- Deploy advanced security tools to prevent cyber attacks, which seek to steal personal data, especially banking or payment card details, or to disrupt access to systems

Responsibilities of Those Engaged in Marketing, Promotion and Events Management

- Ensure that privacy statements attached to emails and other marketing/publicity material meet the requirements of GDPR
- Take care when relying on "opt-in" consent. Do not use "opt-out" consent. Ensure that further consent is requested with each follow-up email, as required. Only retain any personal data for marketing for at most 1 to 2 years.
- Channel data protection queries from clients, target audiences or media outlets to the DPO for advice
- Coordinate with the DPO to ensure all marketing initiatives (e.g. email harvesting) adhere to data protection laws and the OPW's Data Protection Policy
- Ensure that when photographs or videos are to be taken at OPW-organised events where individuals may be identified, attendees are notified in advance that such photography may take place, are made aware of its purpose and are given an opportunity to object, if they wish

Accuracy and Relevance

- We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose.
- Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO.

Data Security

- You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, they must be contractually obliged to guarantee that they will implement appropriate technical and organisational measures to protect the data.

Storing Data Securely

- In cases when data is stored on paper, keep it in a secure place where unauthorised personnel cannot access it.
- Printed data should be cross-cut shredded when it is no longer needed
- Electronic data should be protected by strong passwords that are changed regularly.

- Personal data stored on CDs, DVDs, memory sticks or other portable storage devices must be encrypted or password protected. Devices should be locked away securely when they are not being used.
- The DPO must approve any cloud-based service that is being used to process personal data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the ICT Unit's backup procedures
- Mobile devices such as laptops, tablets or smart phones must be encrypted to prevent data loss
- All servers containing sensitive data must be approved and protected by security systems
- All possible technical and organisational measures must be put in place to keep personal data secure

Data Retention

- We must not retain personal data for longer than is necessary. Data cannot be kept forever, or just in case it is needed – it has to be necessary. All personal data items must have a retention period. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. These will be determined when completing the online questionnaires and published in our Record of Processing Activities.

Transferring data internationally

- There are restrictions on international transfers of personal data. You must not transfer personal data outside the EEA or to an international organisation unless:
  - ☐ It is to a country that the EU Commission has decided offer adequate levels of data protection (e.g. Switzerland). Contact the DPO for the current list.
  - ☐ One of the following safeguards is in place:
    - Legally binding and enforceable instruments between public bodies
    - Binding corporate rules
    - Model contracts (with approved standard data protection clauses)
- Using cloud-based or web-based systems could be transferring data abroad
- Always insist on suppliers telling you where the data will be stored.
- Note that the UK will also leave the EEA once it leaves the EU in March 2019.

10. Rights of Data Subjects

Data subjects have rights regarding their personal data which we must respect and comply with to the best of our ability. We must ensure individuals can exercise their rights in the following ways:

1. Right to be Informed

- We must provide privacy statements explaining what personal data we are processing and what we are doing with it. These must be concise, transparent, intelligible and easily accessible, provided free of charge and be written in clear and plain language, particularly if aimed at children. A template privacy statement accompanies this policy.
- We must keep a record of how we use personal data to demonstrate compliance with the need for accountability and transparency

2. Right of Access

- We must enable data subjects to access their personal data and supplementary information
- We must inform data subjects of and verify the legal basis for the processing

3. Right to Rectification

- We must rectify the personal data of a data subject if requested because it is inaccurate or incomplete.

4. Right to Erasure

- We must delete or remove an individual's data if requested and there is no compelling reason for its continued processing.

5. Right to Restrict Processing

- In certain circumstances we must comply with requests to restrict our processing of personal data.
- We are permitted to store personal data if it has been restricted, but not process it further.

6. Notification Obligation

- We must notify recipients of any rectification, erasure or restriction of personal data unless this proves impossible or involves disproportionate effort.
- We must inform data subjects about these recipients if requested

7. Right to Data Portability

- Where the lawful basis of the processing is consent or a contract, we must provide data subjects with their personal data so that they can reuse it for their own purposes or on different services.
- We must provide it in a commonly used, machine-readable format and send it directly to another controller if requested.

8. Right to Object

- We must respect the right of a data subject to object to the processing where this is based on legitimate interests, on the performance of a task carried out in the public interest or on the exercise of official authority vested in the OPW, including profiling.
- We must respect the right of a data subject to object to processing for direct marketing, including profiling.
- We must respect the right of a data subject to object to processing their data for scientific or historical research or for statistical purposes.

9. Rights in Relation to Automated Decision Making and Profiling

- We must respect the rights of data subject to not be subjected to solely automated decision making and profiling which significantly or legally effects them, unless authorised by law, necessary for entering or performing a contract or based on the data subject's explicit consent.
- Where automated decision is necessary for entering or performing a contract or is used based on the data subject's explicit consent, a data subject has the rights to obtain human intervention, to express their point of view, to obtain an explanation of the rationale for the decision and to challenge the decision.

11. Privacy Statements

When to Supply a Privacy Statement

A privacy statement (also known as a privacy notice on websites) states the type of personal data collected by the controller, how it is to be used and what degree of privacy the person who provides the data may expect.

A privacy statement must be supplied at the time the data is obtained directly from the data subject. If the data is not obtained directly from the data subject, the privacy statement must be provided within one month of having obtained the data.

If the data is being used to communicate with the individual, then the privacy statement must be supplied at the latest when the first communication takes place.

If disclosure to another recipient is envisaged, then the privacy notice must be supplied prior to the data being disclosed.

On forms and websites forms where space is limited, use the following text (approved by the AGs) including a link to the appropriate privacy statement:

> *The personal data that you provide to the OPW will be processed and shared in accordance with the law. See http://www.opw.ie/data_protection/<Your-OPW-privacy-statement.pdf>. See Appendix 1 for more details.*

What to Include in a Privacy Statement

A privacy statement must be concise, transparent, intelligible and easily accessible. It must be provided free of charge and must be written in clear and plain language, particularly if aimed at children. A template privacy statement is on Stór. A privacy notice for OPW websites, including a cookie policy, will be available on Stór shortly.

The following information must be included in a privacy statement:

- Identification and contact information of the data controller and the data protection officer
- The purpose of processing the data and the lawful basis for doing so
- The legitimate interests of the controller or third party, if applicable
- The right to withdraw consent at any time, if applicable
- The category of the personal data (only for data not obtained directly from the data subject)
- Any recipient or categories of recipients of the personal data
- Detailed information of any transfers to third countries and safeguards in place

- The retention period of the data or the criteria used to determine the retention period, including details for the data disposal after the retention period
- The right to lodge a complaint with the Data Protection Commissioner's Office, and internal complaint procedures
- The source of the personal data, and whether it came from publicly available sources (only for data not obtained directly from the data subject)
- Any existence of automated decision making, including profiling and information about how those decisions are made, their significances and consequences to the data subject
- Whether the provision of personal data is part of a statutory of contractual requirement or obligation and possible consequences for any failure to provide the data (only for data obtained directly from the data subject)

12. Data Subject Access Requests (DSARs)

What is a Data Subject Access Request (DSAR)?

A data subject has the right to:

- Receive confirmation that their data is being processed
- Access to their personal data
- Receive supplementary information, which should be provided in a privacy statement.

How we Deal With DSARs and Data Subject Rights

We must provide a data subject with the information they request, free of charge, provided that we can verify their identity. This information must be supplied without delay, and within one month of validating their identity. We must supply the information in writing or by electronic means. Where a request is made by electronic means, we must then provide the information by electronic means, where possible, unless the data subject requests otherwise. Information may be provided orally where requested by the data subject, provided that this is technically possible and that their identity can be verified other means.

If complying with the request is complex or numerous requests are made, the deadline can be extended by two months, but the data subject must be informed within one month. You must obtain approval from the DPO before extending the deadline.

Where the request from a data subject is manifestly unfounded or excessive, we can charge a fee (based on the administrative costs involved) or refuse to act on the request. We must inform that data subject of this within one month **and** must be able to demonstrate that the request is manifestly unfounded or excessive. This can only be done with the express permission of the DPO.

The same rules apply to requests to the exercise of other data subject rights. Requests must be fulfilled within one month. There is no charge for the exercise of these rights, unless they are manifestly unfounded or excessive, when we can charge or refuse to act on them as above.

13. How to Deal with Data Subject Rights

What is the Right to Rectification?

Data subjects have a right to have their inaccurate or incomplete personal data corrected on request.

How we Deal With the Right to Rectification

We must correct inaccurate or incomplete personal data on request.

What is the Right to Erasure?

Data subjects have a right to have their personal data erased in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed
- Where consent is withdrawn
- Where the data subject objects to processing and there are no overriding legitimate grounds for the processing
- The personal data was unlawfully processed
- To comply with a legal obligation
- The processing relates to a child

How we Deal With the Right to Erasure

We can only refuse to comply with a right to erasure in the following circumstances:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation which requires processing, for the performance of a task carried out in the public interest or the exercise of official authority
- For public interest reasons in the area of public health
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The establishment, exercise or defence of legal claims
- The general restrictions applying to all data subject rights.

What is the Right to Restriction of Processing?

Data subjects have the right to have the processing of their personal data restricted in the following circumstances:

- While we verify the accuracy of the personal data, where the data subject is contesting its accuracy
- The processing is unlawful, but the data subject wants it restricted instead of erased
- We no longer need the data, but the data subject requires the data for the establishment, exercise or defence of legal claims
- Where the data subject has objected to the processing (see below), while it is verified whether the OPW's legitimate grounds for the processing override the rights of the data subject.

How we Deal With the Right to Restriction of Processing

Restricted personal data can only be stored. It can only by otherwise processed:

- Where the data subject consents
- To establish, exercise or defend legal claims
- To protect the rights of another individual or organisation
- For reasons of important public interest
- We must inform the data subject before lifting a restriction of processing of their data.

OPW Obligation to Notify Recipients of Correction, Erasure or Restriction

If personal data that has to be corrected, erased or restricted has been passed onto other recipients, they must be contacted and informed of their obligation to erase, correct or restrict the data. If the individual asks, we must inform them of those recipients.

What is the Right to Data Portability?

Data subjects have the right to receive a copy of their personal data in a structured, commonly used and machine-readable format. This would normally be a CSV file, although other formats are acceptable. A PDF file is not machine-readable. We must provide this data either to the data subject who has requested it, or to the controller they have requested it be sent to, where this is technically feasible. This right only applies where the processing is automated and is based on either consent or a contract.

What is the Right to Object?

Data subjects have the right to object to the processing of their personal data in the following circumstances:

- At any time, on grounds relating to their particular situation, where the processing is for:
  - ☐ The performance a task undertaken in the public interest
  - ☐ The exercise our official authority or
  - ☐ Our legitimate interests.
- At any time, where the processing is for direct marketing. We must then cease the processing.
- Where the processing is for scientific or historical research purposes, unless it is necessary for the performance of a task undertaken for reasons of public interest

How we Deal With the Right to Object?

We must always explicitly inform the data subject of their right to object at the first point of communication with them, i.e. in the privacy statement. When providing online services, we must offer an automated way for data subjects to object online.

Where data subjects object to the processing of their personal data:

- Where the processing is based on:
  - ☐ The performance a task undertaken in the public interest, or
  - ☐ The exercise our official authority, or
  - ☐ Our legitimate interests.

  We must cease the processing unless:

  - ☐ We can demonstrate compelling legitimate grounds for processing which override the interests, rights and freedoms of the individual
  - ☐ The processing relates to the establishment, exercise or defence of legal claims
- Where the processing is for direct marketing, we must then cease the processing.
- Where the processing is for scientific or historical research purposes, we must cease processing unless it is necessary for the performance of a task undertaken for reasons of public interest.

The Right not to be Subject to Automated Profiling or Decision Making

Data subjects have a right not to be subjected to decisions based solely on automated processing, including profiling. We may only carry out solely automated profiling or decision making that has a legal or similarly significant effect on a data subject in the following circumstances:

- It is necessary for the entry into or the performance of a contract
- Based on the individual's explicit consent
- It is authorised by law, which provides safeguards for the data subject's rights, freedoms and legitimate interests.

Other than when authorised by law, where using automated profiling or decision making, we must safeguard the data subject's rights, freedoms and legitimate interests. To do so, we must:

- Explain how the automated decision was made
- Allow a data subject to have human intervention in the decision-making
- Allow a data subject to express their point of view regarding any decision about them
- Allow a data subject to contest the decision.
- Carry out regular checks and user testing to ensure our systems are working as intended.

14. Processors

Using Processors

As the OPW is a controller, we must have binding, written contracts (or other legal instruments) in place with any processors that process personal data on our behalf. The contract must contain specific clauses as set out in the GDPR.

We must only appoint processors who can provide sufficient guarantees that their processing will comply with the GDPR and will protect the rights of data subjects. We can be found jointly and severally liable for failures of our processors to abide by the GDPR.

Contracts

Our contracts with processors must comply with the GDPR. They must set out the subject matter and duration of the processing, the nature and stated purpose of the processing, the types of personal data and categories of data subject, and the obligations and rights of the controller.

At a minimum, our contracts must include terms that specify that the processor will:

- Act only on our written instructions
- Ensure that those involved in processing the data are subject to a duty of confidence
- Take all measures to ensure the security of the processing
- Only engage sub-processors with the prior written consent of the controller and under the same obligations as the processor
- Assist the controller in dealing with Data Subject Access Requests and allowing data subjects to exercise their rights under GDPR
- Assist the controller in meeting its GDPR obligations in relation to the security of processing, notification of data breaches. implementation of Data Protection Impact Assessments and prior consultation with the DPC regarding high risk processing
- Delete or return all personal data at the end of the contract
- Submit to regular audits and inspections, and provide whatever information is necessary to demonstrate their compliance with the GDPR to the controller.

15. Criminal Offences and Convictions

Vetting

All data relating to criminal convictions and offences (known as Article 10 data) is a special category of personal data. It must be treated with special consideration both due to its sensitivity and to the level of risk that it presents to its data subjects. The processing of Article 10 data (e.g. vetting, security clearance, Garda clearance) must have a legal basis. This requires that the fundamental rights and freedoms of the data subject be safeguarded and that it is processed under the control of official authority for at least one of the following purposes:

- The administration of justice
- Exercising of regulatory, authorising or licensing functions
- Determining eligibility for benefits or services
- Regulating professions to protect the public from dishonesty, malpractice, improper conduct or incompetence
- Enforcement to prevent, detect or investigate breaches of the law
- Archiving in the public interest, statistical purposes and scientific or historical research.

  As the OPW is not generally involved in these activities, this does not provide a legal ground for vetting of the staff of contractors or subcontractors

- The data subject has given explicit consent to the processing for specified purpose(s). Data subjects sign the Garda vetting form giving their consent for the vetting by the Garda National Vetting Bureau (NVB). This consent cannot be relied on by the OPW as it is a consent given to the NVB and not to the OPW.
- The processing is necessary and proportionate:
    - For the performance of a contract to which the **data subject** is a party. We can vet our own staff as we have contracts of employment with them. We have contracts with contractors, but we do not have a contracts with contractors' staff, sub-contractors or sub-contractors' staff.
    - In order to take steps at the request of the **data subject** before entering into a contract. We can vet prospective OPW employees, but not those of others.
- The processing is necessary for the purposes of:
    - Providing or obtaining legal advice
    - Legal claims or proceedings, or prospective legal claims or proceedings
    - Establishing, exercising or defending legal rights

- The processing is necessary to prevent injury or damage to anyone, loss or damage to property or to protect the vital interests of anyone. This only applies to people (including the data subject) and their property. It does **not** apply to organisations.
- The processing is permitted by law, as is the case for vetting for child protection.

In vetting our staff, we cannot force them to apply for vetting themselves and to then hand over their vetting disclosure to us.

Only an OPW liaison person, who is the sole point of contact with the National Vetting Bureau, should handle any OPW vetting. No one bar the data subject, the Chairman, the Director of Corporate Services, the Head of Human Resource Management, Established and Operational Personnel Managers, the DPO and the OPW liaison person dealing with the data subject's vetting should have access to vetting forms or disclosures.

The liaison person sends vetting forms to the NVB in batches. They may store the vetting forms while building up a batch, typically comprising 50 forms, but they must be stored securely at all times. The liaison person may keep copies of vetting forms after sending a batch to the NVB, but once a vetting disclosure has been received from the NVB for a data subject, their vetting form should be securely destroyed, as its purpose, to enable vetting by the NVB, is now at an end. We no longer have a purpose to process the vetting form, which contains personal data including all names (maiden names or previous names), date of birth, all addresses since birth and any self-disclosed convictions.

When the NVB returns a vetting disclosure, the liaison person must provide a copy to the data subject as soon as possible. In most cases, vetting discloses that the data subject has no convictions or pending convictions. Where this is the case, the liaison person should record that the data subject has cleared vetting and securely destroy any other copies of the vetting disclosure, as its purpose was to reveal that person's convictions. Vetting is a snapshot in time and will need to be repeated regularly.

Where vetting reveals that the data subject has convictions or pending convictions, the liaison person should send the vetting form and disclosure to either the Established or the Operational Personnel Manager for decision, as appropriate.

For child protection vetting, not all convictions represent a threat to children or vulnerable persons, e.g. driving offences. Where vetting is conducted for a specific purpose, such as child prevention, the disclosure of convictions or pending convictions for offences not relevant to child protection, e.g. driving offences, cannot be used for other purposes such as removing a data subject from driving duties or to taking any other disciplinary action against them.

The Personnel Officer must make a judgement call on whether a data subject should clear vetting. The decision should be based on the seriousness and nature of the offence, how recently it occurred and if the disclosure reveals convictions or pending convictions other than those disclosed by the data subject on the vetting form or previously to HR. If the Personnel Officer decides that the data subject can clear vetting, they should inform the liaison person, who will record that the person has passed vetting and securely destroy the vetting form and vetting disclosure. If the Personnel Officer decides that the data subject cannot clear vetting, they should inform the liaison person, who does not record anything. The Personnel Office should retain the vetting form and the vetting disclosure on the data subject's personnel file, as it will be needed as evidence should it be necessary to take disciplinary action against the data subject over the criminal convictions.

Why does the liaison person not record anything? The OPW cannot keep a register of criminal offences and convictions, but it can retain a list of those without such convictions.

Where sections have vetting forms or disclosures on file, without a very strong business justification approved by the DPO, such material should be securely destroyed with immediate effect. You must have approval from the DPO prior to carrying out vetting, clearances or any other processing of Article 10 data.

16. Drones

Introduction

Drones are aircraft without an on-board human pilot, flown by a remote operator. They are also known as Unmanned Aerial Vehicles (UAVs). Civil use of drones is recent, but they offer benefits to the OPW in areas such as infrastructural or watercourse surveying, low cost aerial photography, delivery of payloads to remote or high sites and the detection of new archaeological sites. Unfortunately, the irresponsible use of drones by a minority of domestic users has given rise to concerns about both the risks they pose to aircraft and of intrusions into peoples' privacy. Drones can be used with a variety of different sensors including high-definition still and video cameras, thermal imaging sensors, GPS devices, LIDAR, altimeters, motion detectors and radio-frequency equipment.

Camera-equipped drones (with still or video cameras) are subject to the OPW CCTV Systems Data Protection Policy. If there is sufficient usage of drones within the Office, the DPO will develop a separate Drone Privacy Statement and a Drone Data Protection Policy, as the purposes for which drones are used differs from those of CCTV systems.

The use of drones is not permitted at National Monument sites.

Anyone operating or using a drone for, or on behalf of the OPW must comply with the Irish Aviation Authority (IAA) regulations on drone usage. Drones over 1kg in weight or which may be flown higher than 15m (regardless of weight) must be registered with the IAA. Drones may not be flown where they pose risks to other aircraft, within 5km of an airfield, over 300m from the operator or at altitudes higher than 120m.

Proportionality - What Data can be Captured?

The data gathered by a drone should be limited to what is strictly necessary to achieve a specific purpose (s). For example, a camera-equipped drone used to take aerial landscape photographs should not record images of people. In practice, minimising the collection of personal data can be achieved by using a lower resolution camera, using photographs instead of video, using a live stream rather than recording or not using a camera at all for heat or measurement surveys.

Drone operators must be aware of how a drone operates and how it collects data. Data captured may become personal data if it is combined with other data. Non-camera sensors may record non-personal data that when combined with other data may identify individuals.

Transparency – Notifying the Public

Individuals may not be aware that a drone is recording them or that a drone is equipped with recording equipment. The OPW must do as much as possible to indicate that recording is taking place, by whom, for what purpose and with whom the data may be shared.

The information should be made clear to the public in the area in which the drone will be operated via conspicuous signage, advertising posters, leaflet handouts, social media, local newspaper and media campaigns, to ensure individuals are adequately and clearly informed before and during the flight. The information must accurately describe the dates and times of flights, the flight path and the types of personal data (e.g. imagery, geometry, location, etc.) that may be collected, along with the contact details of the operator and the OPW. Fair processing information on the upcoming and past uses of drones should be made available to data subjects on the OPW website. Drones should be visible and noticeable, using bright colours, flashing lights, sirens or buzzers and visually identifiable, marked with OPW and operator logos. The drone operator (pilot) should also be clearly identifiable, with signage identifying them as the person responsible for the drone.

Processors

Where an OPW processor operates a drone, this processing should be governed by a contract that requires the processor to act only on instructions from the controller.

Storage and retention

Personal data should not be kept in an identifiable form for longer than necessary for the purposes for which they were obtained. The OPW must be able to justify this retention period. Drone pictures or video footage containing personal data that is no longer needed, or that has been inadvertently captured should be deleted. Alternatively, it may be anonymised by blurring or pixelating faces or registration numbers.

Security

Any data captured should be stored in an appropriately secured environment. Access to the data should be controlled, logged and monitored. This may mean storing imagery or footage on a secure or encrypted medium and making it available only to authenticated and authorised users.

Where a drone operator is undertaking work on behalf of the OPW, the personal data captured by the drone should be secured while it is in their possession. None of this data should be retained after it has been handed over to the OPW. Personal data transmitted (live streamed) by a drone to a "base station" must also be similarly secured. Operators and controllers should remain vigilant about eavesdropping, remote control interference and other forms of possible attack on a remotely operated drone.

Should a data breach take place, where there is unauthorised access to or capture of this personal data, a drone operator working on behalf of the OPW should notify the OPW as soon as possible. On becoming aware of such a breach, any OPW staff member must notify the DPO immediately, as we have only 72 hours to report a data breach.

Other Practical Steps for Data Protection Compliance When Using Drones

- Drones should not be used by or on behalf of the OPW for covert surveillance under any circumstances.
- Consider mechanisms that automatically blur faces that are inadvertently filmed during a data collection, or other means to ensure that unintended capture of personal data is avoided, or removed before further processing occurs
- Use software that automatically deletes the remaining personal data collected once the task is completed
- All the data subject rights outlined in Section 12 of this document also apply to data subjects whose data is captured by a drone. Data subjects should be permitted to exercise these rights in respect of drone footage.
- Where an Garda Síochána seek drone footage in relation to a criminal investigation, the same rules apply as for CCTV footage, as set out in the OPW CCTV Systems Data Protection Policy.

17. Data Audits, Monitoring, Compliance and Training

Data Audits

The DPO will carry out regular data audits to manage and mitigate risks and inform compliance with this policy, the GDPR and the Data Protection Acts 1988 to 2018.

Monitoring

Everyone must observe this policy, the GDPR and Data Protection Acts 1988 to 2018. The DPO has overall responsibility for this policy. The OPW will keep this policy under review and amend or change it as required. You must notify the DPO of any infringements of this policy. You must comply with this policy fully and at all times.

Compliance

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk. Such failures are infringements.

Any actual or suspected infringements of this policy or of data protection laws must be reported to the DPO as soon as practically possible.

All members of staff have an obligation to report actual or potential infringements to the DPO. Any member of staff who fails to notify the DPO of an infringement or is found to have known or suspected a infringements has occurred, but has not followed the correct reported this to the DPO may be liable to disciplinary action.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO.

Training

You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested. If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

If you require additional training on data protection matters, contact the DPO.

18. Reporting Data Breaches

Any loss, theft or destruction of personal data by the OPW or its processors, accidental or otherwise is a data breach. Some examples are:

- Sending an email containing personal data to the wrong recipient, particularly if external.
- The loss or theft of unencrypted mobile device such as phones, tablets or laptops
- The loss or theft of a desktop PC or a server
- A cyber-security incident, e.g. hacking, denial of service or data theft.

It is **mandatory** for the OPW to report any personal data breaches to the Data Protection Commission (DPC) **within 72 hours**. This time limit starts from the moment when any OPW staff member **first becomes aware** of the data breach. The DPO is the point of contact with the DPC. All members of staff must I**mmediately** report any actual or suspected data breaches **to the DPO** (or one of his or her staff). This applies even if:

- You are unsure if a data breach has occurred, or
- More investigation is needed to confirm if a breach has actually occurred or to determine its nature and extent.

Why report data breaches to the DPO? There are three reasons for this:

- Mandatory notification of the breach to the Data Protection Commission
- Investigation of the data breach and taking remedial action where necessary
- Maintenance of an OPW data breach register.

The DPO will report the data breach to the DPC as necessary. The DPO has reported the majority of OPW data breaches notified to date. There have been no consequences for any breaches reported to date (as they were minor). There **are** consequences for failure to report data breaches or for late reporting. The DPO will update breach reports to the DPC, where:

- A suspected breach turns out not to have been a breach or
- There is new information regarding the nature and extent of the breach

The business area responsible for the breach must also notify any affected data subjects as soon as possible, where a data breach may present a risk to data subjects , e.g. a loss of payment card data putting them at risk of fraud.

Any member of staff who fails to notify the DPO of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures may be liable to disciplinary action.

19. OPW Data Protection Registers

Register of Processing Activities

As a controller, the OPW must maintain an ongoing record of its processing activities. This register will contain details of all personal data processing activities undertaken by the OPW. Online questionnaires are used to compile and maintain the register. As the DPO developed the questionnaires, the Data Protection Unit is co-ordinating the completion process. As this is a legal obligation, which also provides the information needed for other legal obligations, **all** staff and business units must cooperate with this process by completing these questionnaires accurately and as soon as possible. Failing to do so is contravenes both European and Irish data protection law and puts both the OPW in legal jeopardy.

This register will include:

- Name and contact details of the controller (if applicable, joint controller or controller's representative)
- Name and contact details of the data protection officer
- The purposes of the processing
- Description of the categories of data subjects
- Description of the categories of personal data
- Categories of recipients to whom the personal data has/will be disclosed (including third countries or international organisations)
- If applicable, transfers of personal data to a third country/international organisation (including their identity and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards)
- If possible, the envisaged time limits for erasure of the different categories of data
- If possible, a general description of the technical and organisational security measures referred to in Article 32(1)

Register of Personal Data Repositories

This will include a list of databases, applications, file shares, tambour units, storerooms, filing cabinets, off-site archives, motorised shelving and other data repositories containing personal data. It is compiled and maintained by the use of online questionnaires as part of the process above. Again, these questionnaires should be completed accurately and without delay.

Register of Personal Data Breaches

This register is compiled by the DPO as staff report potential data breaches to him or her. It records details of all data breach incidents or potential incidents, even where these are not reported to the DPC. The DPC may inspect this register during an audit to ensure that the OPW is complying with the requirements of the GDPR for mandatory reporting of all data breaches.

Register of Data Subject Access Requests

As Data Subject Access Requests (DSARs) are received, the DPO compiles a register of those making the requests. This is necessary to determine if requests are excessive or repetitive. This contains:

- The requester's contact details and, where applicable, those of their solicitor
- The date that the DSAR was received and the date that the receiver's ID was verified. The deadline for reply is normally one month from the latest of these dates.
- A list of the forms of ID used to verify the requester's identity. Copies of ID documents are not retained once the requester's identity has been verified,
- The dates of the initial and any interim replies
- The dates of any request for additional material and the deadline for this additional reply
- The dates of partial and final DSAR fulfilment
- If the OPW had no data to fulfil the DSAR
- Copies of correspondence with the requester or their solicitor. The personal data sent to the requester is not retained, unless it is could be required as part of a legal claim.

Appendix 1 – Data Protection Principles

Data Protection Principles

Compliance with the data protection principles is essential for lawful processing of personal data by the OPW, as they are legal requirements under Articles 5 and 6 of the General Data Protection Regulation (GDPR) and Section 71 of the Data Protection Acts 1988 to 2018.

1. Lawful, Fair and Transparent Processing of Personal Data

Article 5.1(a) of the GDPR states that personal data shall be processed lawfully, fairly and transparently in relation to the data subject. ***This is the principle of lawfulness, fairness and transparency, one of the eight Data Protection principles.*** Section 71(1)(a) of the Data Protection Acts 1988 to 2018 states that personal data shall be processed lawfully and fairly.

1.1. How can Personal Data be Processed Lawfully?

The lawful grounds for processing personal data are in Article 6 of the GDPR. Processing of personal data is only lawful if at least one of the following grounds is true, but note that not all are available to a public authority like the OPW:

1.1.1. Consent of the Data Subject to the Processing of their Personal Data for One or More Specific Purpose(s)

Consent should be given by a clear affirmation that a freely given, explicit, specific informed and unambiguous indication of a data subject's agreement to the processing of their personal data, either in writing (including electronically) or orally (during a phone call). For example, consent can be given by a signature, by ticking a box on a form or a website, or by choosing a technical setting in an app, amongst other ways. Silence, pre-ticked boxes or inactivity are not consent, which must be opt-in not opt-out.

Consent should cover all processing activities carried out for the same purpose(s), but multiple purposes require separate consents. Consent for the purpose of recruitment would cover processing of a data subject's CV and interview notes. It would not cover adding their personal data to the payroll, as this is a separate purpose.

For consent to be informed, the data subject must be aware of both the identity of the controller and the intended purpose(s) of the processing.

Consent is not freely given where the data subject has no genuine or free choice or cannot refuse or withdraw their consent without detriment. It is not freely given if a contract is conditional on a consent to process personal data that is not necessary to fulfil that contract.

Consent cannot be used where a clear imbalance exists between the data subject and the OPW, especially in its roles as a public authority or as an employer, as it is therefore unlikely that consent was freely given in all circumstances of that specific situation. Where processing is based on consent, the OPW must subsequently be able to demonstrate the data subject's consent. If this consent is given in a written declaration that also covers other matters, for it to be binding, the request for consent must:

- Be clearly distinguishable from other matters
- Be intelligible and easily accessible
- Use clear and plain language.

The use of consent as a lawful basis for data processing by the OPW is not totally excluded under the legal framework of the GDPR and it can be appropriate under certain circumstances. For example, the OPW may wish to collect email addresses to send marketing information on its heritage sites. This is possible, provided that there is no obligation to participate and that the OPW asks for consent to use email addresses for this (exclusive) purpose. Those that do not consent will not miss out on any core service of the OPW or the exercise of any right, so they are able to freely give or refuse their consent to this use of data.

All the information on heritage sites and events is also available on the OPW's heritage website. Care should be taken not to retain these addresses for longer than 1 - 2 years. Each email sent should ask for consent on an opt-in basis to send further marketing emails. Be careful about offering prizes or running competitions in return for seeking personal data, as this could be seen as an inducement. The consent might not be seen as freely given, as the data subject loses out if they do not consent. Where prizes are offered or competitions run, a separate consent should be sought for entry into the draw or competition.

It should be as easy to withdraw consent as to give it. A data subject can withdraw their consent at any time. This limits the usefulness of consent, as it must be actively managed. Withdrawal of consent does NOT affect the lawfulness of processing prior to its withdrawal. Data subjects should be informed of this prior to giving consent. Consent is addressed by GDPR Articles 6 – 8; GDPR Recitals 32, 33, 42, 43, 58 and by Sections 71(3) and 71(4) of the Data Protection Acts 1988 to 2018.

1.1.2. Contractual Necessity Where the Data Subject is a Party to the Contract

This ground can also be used at the request of the data subject prior to entering into a contract. A typical example would be a tender containing the CVs and educational qualifications of the tenderer's staff, which are personal data. The processing of this personal data from all the tenderers is lawful under this ground, even though only the successful tenderer will be awarded a contract. Most of OPW's functions in relations to property management and procurement are also covered by this ground. GDPR Article 6.1.b deals with contractual necessity.

1.1.3. Non-Contractual Legal Obligation on Controller

This requires a legal basis in EU or Irish law, which imposes an obligation on the OPW, determines the purpose of the processing and which is proportionate to the legitimate aim pursued. The specific statute(s) must be stated, but it does not need to refer to data protection. For example, the Phoenix Park Act, 1925 allows the OPW to licence a person to have exclusive use of part of the park and charge admission, e.g. Bloom or concerts. This provides the legal basis for the OPW to process the licensee's personal data, despite predating the Data Protection Acts by six decades.

Unlike the Revenue Commissioners or the Department of Employment Affairs and Social Protection, most of the OPW's functions are administrative and they are not set out in detail in Irish or EU law. Section 38(1)(b) of the Data Protection Acts 1988 to 2018 provides that processing personal data is lawful, where this is necessary for the administration by a controller of any non-statutory scheme, programme or funds, where the legal basis for such administration is a function of a controller conferred by law or by the Constitution. In addition, Article 28(2) of the Irish Constitution, Bunreacht na hÉireann and the Ministers and Secretaries Acts 1924 to 2017 bestow overall powers on the Government to collect and process data.

1.1.4. Protection of the Vital Interests of the Data Subject or Another Natural Person

This ground protects the vital interests of living individuals, but is not generally of use for other processing by a public body.

1.1.5. Performance of a Task Carried Out in the Public Interest or in the Exercise of Official Authority Vested in the Controller

This requires a legal basis in EU or Irish law, which meets an objective of public interest and which is proportionate to the legitimate aim pursued. The specific statute(s) must be stated, but it does not need to refer to data protection. For example, the National Monuments Act, 1930 requires the finders of archaeological objects to report the find, giving their name and address. This provides the legal basis for processing the finder's personal data, even though the Act does not mention data protection.

Unlike the Revenue Commissioners or the Department of Employment Affairs and Social Protection, few of the functions of the Commissioners of Public Works in Ireland are set out in detail in Irish law. Section 38(1)(b) of the Data Protection Acts 1988 to 2018 provides that processing personal data is lawful, where this is necessary for the administration by a controller of any non-statutory scheme, programme or funds, where the legal basis for such administration is a function of a controller conferred by law or by the Constitution.

In addition, Article 28(2) of the Irish Constitution, Bunreacht na hÉireann and the Ministers and Secretaries Acts 1924 to 2017 bestow overall powers on the Government to collect and process data. Section 38(4) of the Data Protection Acts 1988 to 2018 provides that the Minister for Public Expenditure and Reform may make regulations for the processing of personal data necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Commissioners of Public Works in Ireland.

1.1.6. Legitimate Interests Pursued by the Controller or a Third Party

This does not apply to processing carried out by public authorities in the performance of tasks carried out in the public interest or in the exercise of official authority vested in them. It applies to tasks that are non-core, not set out in legislation and in the interests of the public body and not in the public interest, such as security. The OPW uses this as grounds for processing personal data with CCTV systems.

1.2. How can Personal Data be Processed Fairly?

To process personal data fairly, data subjects must be told in advance of the purpose(s) for which their personal data is being processed, where the personal data is obtained directly from the data subject, whether this is in person, by phone, by means of a form or via a website. OPW RFTs should state what personal data is being processed and the purposes for which this is being done. All the purpose(s) for which the OPW processes personal data should also be stated both in the OPW Privacy Statement(s) and the Record of Processing Activities required under Article 30 of the GDPR.

Layered privacy statements should be used, providing simple and clear information at first and adding additional information in each successive layer. Where, for example, it is not possible to state the purpose(s), for reasons of space or complexity, the following summary privacy statement should be used to either verbally inform the data subject or it should be stated on the form or website:

The personal data that you provide to the OPW will be processed and shared in accordance with the law. See: *See http://www.opw.ie/data_protection/<Your-OPW-privacy-statement.pdf>*.

This is the lowest and least detailed level of privacy statement. The URL referenced in it links to the next highest (intermediate) level. This should contain all the purpose(s) for which the personal data is being processed. It must also contain a link to the full OPW Privacy Statement(s). This in turn must contain all the information required under Article 13 of the GDPR. Where the personal data has not been obtained from the data subject, the additional information required under Article 14 should be included in the OPW Privacy Statement(s). This, which should also contain the information required under Article 13, must be provided to the data subject within one month or, if used for communication, no later than the time of first communication, or before being used for any further purpose.

While the OPW Privacy Statement(s) document states these purposes, it would be both unfair and entirely unreasonable to expect a data subject to read the privacy statement on the OPW's website before visiting an OPW heritage site or entering an OPW building. However, to ensure that data subjects have access to it, at least ten copies of the privacy statement should be kept at the reception of all OPW sites and buildings.

1.3. How can Personal Data be Processed Transparently?

Before a data subject's personal data can be processed, they must be informed:

(a) that their data will be processed and

(b) of the purposes for which their personal data will be processed.

The OPW Privacy Statement(s) provides these purposes, along with all the other information that the OPW must give to data subjects under GDPR Article 13. It would be both unfair and entirely unreasonable to expect data subjects to read this document on the OPW website before visiting an OPW heritage site or entering an OPW building. However, at least ten copies of the privacy statement should be held at the reception of all OPW sites, and given to data subjects on request.

2. Purpose Limitation for Processing of Personal Data

Article 5.1(b) of the GDPR states that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in any way incompatible with those purposes. ***This is the purpose limitation principle.***

Personal data can only be processed for the purposes specified in the OPW Privacy Statement(s). If personal data is to be processed for additional purposes, these must be approved in advance by the OPW's Data Protection Officer and, if necessary, by the Data Protection Commission. The OPW Privacy Statement(s) and the OPW Record of Processing Activities must then be amended.

3. Minimisation of personal data

Article 5.1(c) of the GDPR states that personal data processed shall be adequate, relevant and limited to what is necessary. In other words, it should process only the minimum personal data necessary and be proportionate. ***This is the data minimisation principle.***

When processing personal data, the purposes for which the personal data is to be processed must be balanced against the risk to the rights and freedoms of data subjects in relation to the protection of their personal data.

4. Accuracy of personal data

Article 5.1(d) of the GDPR states that personal data collected shall be accurate and, where necessary, kept up to date. Every reasonable effort must be taken to ensure that personal data that are inaccurate, regarding the purposes for which they are processed, are erased or rectified without delay. ***This is the accuracy principle.***

For example, as payments are now made by Electronic Funds Transfer (EFT), it is vital that inaccurate bank account details be corrected as soon as possible to ensure that payments reach the intended recipient. Correcting an inaccurate postal address would be of less importance as these are no longer used for processing payments. While they were formerly used for mailing cheques, postal addresses now serve the secondary function of helping to identify the correct recipient, If they are not used for this purpose, inaccurate postal addresses should be erased. If, on the other hand, the postal address was the only means of contacting the data subject, then it would be essential to correct it as soon as possible.

5. Retention of Personal Data

Article 5.1(e) of the GDPR states that personal data collected shall not be kept in an identifiable form for longer than necessary for the purposes for which it is processed. ***This is the principle of storage limitation.***

Personal data can attract Data Subject Access Requests (DSARs) from individuals seeking copies of their personal data. Under the previous legislation, DSARs required the payment of a fee of €6.35 and had a 40 day time limit. Under the GDPR, from 25 May 2018, no fee is payable for a first DSAR and it must be fulfilled within 30 days. In fulfilling DSARs, the OPW cannot release the personal data of other data subjects, so anything that identifies or makes another individual identifiable must be redacted. The longer we keep personal data, the greater the volume of material to be gone through in a tight frame for DSARs (or other requests for data subject rights).

Section 60 of the Data Protection Act 2018 provides for restriction of the GDPR data subject rights where this is necessary and proportionate for the establishment, exercise or defence of actual or prospective legal claims and proceedings, whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure. For example, this allows the OPW to withhold personal data from a DSAR where this material is being used by the OPW in a court case.

Where the OPW is involved, or may be involved in any legal action, the relevant personal data should be retained for the duration of the case and any follow up appeals.

6. Security of Personal Data

Article 5.1(f) of the GDPR states that personal data collected shall be processed in a manner that ensures appropriate security, using appropriate technical and organisational measures, to protect it from:

- Unauthorised or unlawful processing
- Accidental Loss
- Disclosure
- Destruction

This is the principle of integrity and confidentiality.

It is vital that security precautions are taken to prevent unauthorised people from having access to view, copy or modify personal data. Access should be restricted to authorised personnel only.

IT systems which process personal data should be password protected with each authorised user having their own named login. Access should be automatically logged (user name, login and logout dates and times).

Manual filing systems should be kept locked when not in use, with the key removed and locked away securely. For manual filing systems where automatic logging is not possible, keep a written log of those who access the filing system. Note that papers containing personal data which are intended to form part of a filing system are also covered by the GDPR, e.g. papers kept in a folder on your desk which will be filed when no longer in daily use. Under OPW's Secure Desk Policy, you should not leave any papers or files containing personal data on your desk when you are not present. Such papers/files should be locked away in a press or filing cabinet with the key removed, and locked away securely. Your PC/laptop screen should be locked with <Windows>-L whenever you leave your desk. While all this seems a nuisance, if done consistently, it will become habitual and automatic good data protection practices.

Under GDPR Article 5.1(f), the OPW **cannot** disclose a data subject's personal data to others. When responding to Data Subject Access Requests by supplying the data subject with a copy of their personal data, take particular care to redact the personal data of others before supplying the material to the data subject. Do **NOT** show or give anyone unredacted personal data as this may contain the personal data of or otherwise identify other data subjects.

Personal data should always be backed up, where possible, so that it can be recovered in the event of its loss or destruction.

7. Accountability for Personal Data Processed by the OPW

Article 5.2 of the GDPR states that as a controller, the OPW is responsible for and must be able to demonstrate compliance with all of the principles from sections 6.1 to 6.5. ***This is the principle of accountability.*** Article 24 further states that the OPW must take account of the risks to data subjects involved in processing personal data and implement must appropriate technical and organisational measures to ensure that we comply with the GDPR and to be able to demonstrate this compliance. It is not enough to say that our processing of personal data complies with GDPR – we must be able to prove it.

How can this be achieved?

The OPW must:

- Have a Data Protection Policy (this document) and must implement it (Article 24).
- Establish internal data protection assessment procedures before creating new systems which process personal data or where existing processing presents a high risk to the rights and freedoms of data subjects.
- Map its systems, including manual ones, to identify all personal data processing activities and maintain an inventory of them (Article 30).
- Have a Data Protection Officer and other individuals with responsibility for Data Protection in general (Articles 37-39).
- Provide adequate and specific Data Protection awareness, training and education to staff regarding the correct and legal processing of personal data (Article 39).
- Allocate sufficient resources for Privacy Management and Data Protection. This includes training, budget and staffing. (Article 38).
- Set up transparent procedures to manage Data Subject Access Requests (DSARs) and requests for correction or deletion.
- Establish an internal complaints handling mechanism.
- Set up internal procedures to effectively manage and report security breaches involving personal data (Articles 33-34).
- Undertake Data Protection Impact Assessments in specific circumstances, for new types of processing or where the processing of personal data presents a high risk to the rights and freedoms of data subjects (Article 36).
- Undertake regular Data Protection Audits to ensure that all these measures are being implemented and are working in practice (Article 39).

8. Exercise of Data Subject Rights

Allowing data subjects to exercise their rights as set out in section 9 of this policy may be considered to be an eighth Data Protection Principle.