An tÚdarás Slándála Príobháidí
The Private Security Authority

The Security Regulator

Private Security Authority

Data Retention Policy

January 2023

Contents **Page number**

1. Introduction

The Private Security Authority is committed to protecting the right and privacy of individuals in accordance with the EU General Data Protection Regulation, 2016/679 (GDPR).

Data Protection is the manner in which the privacy rights of individuals are safeguarded in relation to processing their Personal Data. Personal Data covers **any** information that relates to an identifiable, living individual. The data can be electronic, manual and images and may be held on computers or manual files. The policy applies to all Data Subjects whose personal data is held by the PSA, from staff details to clients and members of the public.

The core Principles of Data Protection which are to be upheld by the PSA are to:

1. Process it lawfully, fairly, and in a transparent manner;
2. Collect it only for one or more specified, explicit and legitimate purposes, and do not otherwise use it in a way that is incompatible with those purposes;
3. Ensure it is adequate, relevant and limited to what is necessary for the purpose it is processed;
4. Keep it accurate and up-to-date and erase or rectify any inaccurate data without delay;
5. Where it is kept in a way that allows you to identify who the data is about, retain it for no longer than is necessary;
6. Keep it secure by using appropriate technical and/or organisational security measures;
7. Be able to demonstrate your compliance with the above principles; and
8. Respond to requests by individuals seeking to exercise their data protection rights (for example the right of access).

2. Definitions

Below are definitions of the key terminology, from the website of the Office of the Data Protection Commissioner

Personal data - The term “personal data” means any information relating to a living person who is identified or identifiable (such a person is referred to as a “data subject”). If the information can be used on its own or in combination with other information to identify a specific person, then it counts as personal data.

The GDPR gives examples of identifiers, including names, identification numbers, and location data. A person may also be identifiable by reference to factors which are specific to their identity, such as physical, genetic or cultural factors.

Processing - The term “processing” refers to any operation or set of operations performed on personal data. Processing includes storing, collecting, retrieving, using, combining, erasing and destroying personal data, and can involve automated or manual operations.

Data Protection Commission - The “Data Protection Commission” was established by the Data Protection Acts 1988 to 2018 ('the Data Protection Acts'). Under the GDPR and the Data Protection Acts, the Commission is responsible for monitoring the application of the GDPR in order to protect the rights and freedoms of individuals in relation to processing. The tasks of the Commission include promoting public awareness and understanding of the risks, rules, safeguards and rights in relation to processing, handling complaints lodged by data subjects and cooperating with (which includes sharing information with) other data protection authorities in other EU member states.

Data Controller - A “data controller” refers to a person, company, or other body which decides the purposes and methods of processing personal data. The Private Security Authority is the Data Controller for the PSA.

Data Processor - A “data processor” refers to a person, company, or other body which processes personal data on behalf of a data controller (the PSA).

Consent - Some types of processing are carried out on the basis that you have given your consent. Under the GDPR, consent to processing must be freely given, specific, and informed. You cannot be forced to give your consent, you must be told what purpose(s) your data will be used for and you should show your consent through a 'statement or as a clear affirmative action' (e.g. ticking a box).

Consent is not the only lawful basis on which your personal data can be processed. Article 6 of the GDPR sets out the complete list of lawful reasons for processing personal data as:

1. Consent
2. To carry out a contract
3. In order for an organisation to meet a legal obligation
4. Where processing the personal data is necessary to protect the vital interests of a person
5. Where processing the personal data is necessary for the performance of a task carried out in the public interest
6. In the legitimate interests of a company/organisation (except where those interests contradict or harm the interests or rights and freedoms of the individual)*

*It is important to note that Article 6(1)(f) provides that the "legitimate interests" reason is not available to public authorities where the processing is being conducted in the exercise of their functions.

Data Protection Officer (DPO) - The GDPR requires the PSA to appoint a Data Protection Officer (DPO). The current DPO for the PSA is Keith Nolan of the Corporate Affairs Division.

3. Record Retention Periods

The GDPR places direct data processing obligations on businesses and organisations at an EU-wide level. According to the GDPR, an organisation can only process personal data under certain conditions. For instance, the processing should be fair and transparent, for a specified and legitimate purpose and limited to the data necessary to fulfil this purpose. It must also be based on one of the following legal grounds.

1. The consent of the individual concerned.
2. A contractual obligation between you and the individual.
3. To satisfy a legal obligation.
4. To protect the vital interests of the individual.
5. To carry out a task that is in the public interest.
6. For your company's legitimate interests, but only after having checked that the fundamental rights and freedoms of the individual whose data you are processing are not seriously impacted. If the person's rights override your interests, then you cannot process the data.

To comply with this rule, the PSA policy on retention periods is set at 5 years for all records both electronic* and hard copy.

The PSA is committed to effective records management retention and disposal to ensure that it:

- Meets legal standards in terms of retention periods
- Optimises the use of space
- Minimises the cost of record retention
- Securely destroys outdated records.

In setting the retention schedule, the PSA is mindful to:

- Comply with the relevant legislation
- Avoid trying to accommodate every conceivable need

- Retain information if it is likely to be needed in the future and if the consequences of not having it would be substantial
- Be conservative, avoid inordinate degrees of risk
- Apply common sense
- Ensure systematic disposal of records within a reasonable period after their retention period expires.

**Most of the PSA's electronic data is held on legacy systems maintained on our behalf by the Department of Justice. Because of the nature of these legacy systems it may not be possible to remove all electronic data in accordance with this policy. The PSA is committed to working with the Department of Justice to moving away from these legacy systems so that over time the commitments in this policy can be met.*

4. Disposal of records

All records will be destroyed under confidential conditions. Paper records will be shredded under PSA supervision of a member of the PSA. Data records will be reviewed regularly. IT's policy on data retention to be used to remove unnecessary records.

Appendix A

Exceptions to the 5 year retention policy of the PSA.

Record	Minimum Retention Period	Final Action
Individual Applications – Successful Licence Application	6 years (Two license periods)	Destroy under confidential conditions
Individual Applications – Unsuccessful Licence Application	3 years (Period after which applicant is required to re-sit training)	Destroy under confidential conditions
Individual Appeals – Documentation	7 years	Destroy under confidential conditions
Individual Appeals – Legal Advices	Indefinitely	Not applicable
Electronic Data held by Service Providers – Applications not returned to the PSA	1 year	Destroy / delete under confidential conditions
Electronic Data held by Service Providers – Unsuccessful Licence Application	1 year	Destroy / delete under confidential conditions
Electronic Data held by Service Providers – Successful Licence Application	3 year	Destroy / delete under confidential conditions
Criminal Record Certificate	7 years	Destroy under confidential
Prosecution results	Indefinitely	Not applicable
Garda Vetting Forms	7 years – confirmation notices only	Destroy under confidential conditions

Garda vetting assessment unsuccessful applicants	1 year	Destroy under confidential conditions
Ethics in public office -	15 years in hard copy format only, accessed by CEO/H of CA only	Destroy under confidential conditions
Invoices, VAT records, Bank records	Hold for current year plus 6 years	Destroy under confidential conditions
H&S records – accident reports etc	Hold indefinitely, if contain personal data destroy after 7 years	Destroy under confidential conditions

Invitation to tender docs	3 years after award of contract	Destroy under confidential conditions
Suppliers proposals	1 year after award of contract	Destroy under confidential conditions
Tender report	Hold for 4 years	Destroy under confidential conditions