An tÚdarás Slándála Príobháidí
The Private Security Authority

The Security Regulator

Private Security Authority

Data Protection Policy

October 2019

Contents **Page**

1. Introduction

The Private Security Authority (PSA), established under the Private Security Services Act 2004, is responsible for the regulation of the private security industry. Our role is to protect the public and clients of the security industry by promoting a quality regulatory environment through our licensing system. The PSA licences 35,000 contractors and employees. As a Regulatory Body, our responsibilities include:

- the licensing of individuals and contractors operating in the following sectors:
    - ❖ Door Supervisor (Event Security)
    - ❖ Door Supervisor (Licensed Premises)
    - ❖ Security Guard (Event Security)
    - ❖ Security Guard (Static)
    - ❖ Security Guard (Alarm Monitoring)
    - ❖ Security Guard (CCTV Monitoring)
    - ❖ Access Control (Installation and Maintenance)
    - ❖ CCTV (Installation and Maintenance)
    - ❖ Intruder Alarm (Installation and Maintenance)
    - ❖ Cash In Transit
    - ❖ Private Investigator
    - ❖ Locksmith;
- the monitoring of the provision of security services;
- the specifying of standards and qualifications to be observed in the provision of security services;
- the creation of Public Registers

The PSA necessarily collects, processes and stores significant volumes of personal data from our licensees, staff, service providers and others.

In accordance with the EU General Data Protection Regulation, 2016/679 (GDPR) and given further effect in Part 3 of the Data Protection Act 2018, the PSA is a 'Data Controller' and, as such, has significant responsibilities for ensuring the privacy of data subjects and the protection of personal data processed.

GDPR defines personal data as

"any information relating to an identified or identifiable natural person (data subject)"

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number (e.g. PPSN), location data or online identifier and covers all electronic, manual and image data which may be held on computer or on manual files.

Note: The key definitions used in the GDPR are set out in Appendix A.

2. Scope

This policy applies to all personal data collected, processed and stored by the PSA in

respect of all individuals, (i.e. applicants, licence holders and staff) by whatever means including paper and electronic records.

This Policy takes account of best practice in the area of data protection using resources available on the website of the Office of the Data Protection Commissioner and the European Commission.

3. Data Protection Principles

The six principles of the General Data Protection Regulation (GDPR) require that personal data is:

1. Processed in a way that is lawful, fair and transparent;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
3. Adequate, relevant and is limited to what is necessary;
4. Accurate and kept up to date;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
6. Processed in a manner that ensures appropriate security of the data.

Article 5(2) of the GDPR also obliges the PSA to "*be responsible for, and be able to demonstrate, compliance with the principles*".

Application of Data Protection Principles in the Private Security Authority
GDPR requires that the processing of personal data is conducted in accordance with the data protection principles set out above. The PSA's policies and procedures are designed to ensure compliance with these principles.

3.1 Personal data must be processed in a way that is lawful, fair and transparent[2]

Article 6 of the GDPR allows for the processing of personal data where *'processing is necessary for compliance with a legal obligation to which the controller is subject'*. Section 37(1) of the Data Protection Act 2018 further states that processing is lawful where it is required for *'the performance of a function of a controller conferred by or under an enactment or by the Constitution.'* The majority of personal data processing by the PSA is carried out as part of their legal obligations under the Private Security Services Act 2004.

Occasionally the PSA will carry out the processing of data in the public interest. Article 6.1(e) of the GDPR allows for the processing of personal data where '*processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the* controller'. Table 2 in Appendix B, lists tasks carried out in the public interest by the PSA, for which personal data may also be processed.

In some circumstances the PSA may request the consent of the data subject to process their data. In such cases, consent will be sought at the time that the data is collected and the data subject will be advised that they can withdraw their consent at any stage during processing. The PSA will be fully transparent in relation to how personal data collected is used, in particular ensuring that the data is not used in a way that a data subject would not expect.

3.2 Personal data can only be collected for specific, explicit and legitimate purposes

The PSA processes personal data only for the purposes for which it is collected. Any further proposed processing of data (regardless of apparent compatibility with original purpose) will be the subject of an impact assessment to ascertain if it poses a risk to the rights and freedoms of the data subject. This assessment may take the format of a Data Protection Impact Assessment (see Section 5.5 below)

3.3 Personal data must be adequate, relevant and limited to what is necessary for processing (data minimisation)

The PSA will ensure that the data collected and held is the minimum amount required for the specified purpose. The PSA will not collect personal data unnecessary to the business purpose. All personal data requests issued by the PSA will clearly state the business purpose for the collection of such data.

3.4 Personal data must be accurate and kept up to date

In order to ensure that the functions of the PSA are delivered efficiently and effectively, the PSA will ensure that, where possible, all personal data held is kept accurate and up to date. PSA Divisions holding personal data are responsible for ensuring that all manual/computer procedures are adequately maintained and that, where notified of inaccuracies, the personal data is corrected in a timely manner.

Data subjects have the right to have inaccurate data held by the PSA updated or erased, as appropriate.

3.5 Personal data is only held for as long as is necessary

The PSA will ensure that a data retention policy is in place, which establishes the length of time that personal data is retained and the purpose(s) of its retention. The PSA will ensure that data will not be retained for longer than it is required and will be properly destroyed/deleted when it is no longer needed.

In this regard, it is important to note that the PSA has limited control in relation to record destruction due to obligations which arise under the Freedom of Information Act, 2014.

3.6 Personal data is processed in a manner that ensures appropriate security of the data

The PSA works with the Department of Justice and Equality to maintain the highest standards of technical, organisational and physical security measures. IT systems used by the PSA are managed and maintained by the Department's ICT Division. Service level agreements are in place with the Department and are reviewed and updated as necessary, to provide assurance to the PSA that systems are secure and personal data is protected.

PSA staff have undergone training in relation to their personal responsibilities for the protection of personal data.

4. GDPR – Rights of 'data subjects'

Subject to Section 60 of the Data Protection Act, 2018 and any associated Regulations, the GDPR specifies the following rights for data subjects:

- right to be informed/right of access
- right to rectification
- right to erasure
- right to restrict processing
- right to data portability
- right to object to processing
- rights in relation to automated decision making and profiling.

4.1 Right to be informed and right of access

As noted previously Data Subjects have the right to be informed by the PSA about the collection and use of their personal data. In addition, they have the right to access their personal data and other supplementary information, as appropriate.

The PSA has implemented procedures to ensure that all such Subject Access Requests (SAR) are responded to within the one month period as required under Article 12 of the GDPR.

4.2 Right to rectification

Data subjects have the right to have inaccurate personal data held by the PSA rectified and to have incomplete personal data updated so that it is complete.

On receipt of a request from a data subject for rectification of their personal data, the PSA will take reasonable steps to ensure that the data held is accurate and will ensure that data is rectified, where necessary.

4.3 Right to erasure

Article 17 of the GDPR provides for the right of data subjects in certain circumstances to have their personal data erased ('right to be forgotten'). The right to erasure is not an absolute right and does not apply in circumstances where PSA's processing of personal data is necessary in particular:

- For the performance of legal duties carried out by the PSA or tasks carried out in the public interest (Appendix B, Tables 1&2)
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
- Where the data is required for the establishment, exercise or defence of legal claims.

Where a data subject is of the opinion that elements of personal data held by the PSA is incorrect, they may make a request in writing to have such data permanently erased. The PSA will review all such requests and, where appropriate, will erase the data in question.

4.4 Right to restriction of processing

A data subject has the right obtain a restriction of processing of their personal data where any one of the following applies:

- the data subject contests the accuracy of their data. The restriction will apply for a period enabling the PSA to verify the accuracy of the personal data;
- the processing is unlawful and the data subject does not wish to have the data erased, but rather wishes to restrict its' use;
- the PSA no longer requires the data in question but the data subject seeks its' retention in order to establish, exercise or defend a legal claim; or
- the data subject has objected to the processing of their data by the PSA pending verification from the PSA on whether the legitimate grounds for processing overrides the data subjects concerns.

As a matter of good practice, the PSA will restrict the processing of personal data whilst a review of the accuracy of the data and/or the legitimate grounds for processing the data is carried out. This restriction of processing will take into account any Regulations made under Section 60 of the Data Protection Act, 2018.

4.5 Right to data portability

The collection of a significant proportion of personal data by the PSA is lawful in accordance with Article 6.1(c) of the GDPR i.e. '*necessary for compliance with a legal obligation to which the controller is subject*'.

In cases where the PSA has collected personal data from a data subject by consent or by contract, that data subject can request the PSA to provide the data in electronic format in order to provide it to another Data Controller. The PSA will comply with all such legitimate requests.

4.6 Right to object to processing

Under Article 21 of the GDPR, data subjects have a right to object to the processing of their personal data in specific circumstances. Where such an objection is received, the PSA will assess each case on its' individual merits.

4.7 Right not to be subjected to automated decision making

Data subjects will have the right not to be subjected to a decision based solely on automatic processing, including profiling, that have a legal or similarly significant effect on them.

The PSA does not issue decisions based solely on automatic processing.

4.8 Complaints

Data subjects who may be concerned that their rights under the GDPR are not upheld by the PSA can contact the PSA's Data Protection Officer (DPO). The DPO will engage with the data subject in order to bring their complaint to a satisfactory conclusion.

The DPO can be contacted at info@psa.gov.ie

Where the complaint to the DPO cannot be resolved, the data subject will be informed in writing and will be further informed of their right to bring their complaint to the Data Protection Commission.

5.0 Responsibilities of the Private Security Authority

The PSA is responsible for the following:

5.1 Implementing and maintaining appropriate technical and organisational measures for the protection of personal data.

The PSA, together with the Department of Justice and Equality have implemented appropriate technical and organisational measures to ensure that all data held under its control is secure and is not at risk from unauthorised access, either internal or external. Measures for the protection of personal data are reviewed and upgraded, where appropriate, on an ongoing basis.

5.2 Maintaining a record of data processing activities

The PSA maintains [s3]a written record of all categories of processing activities for which it is responsible in accordance with GDPR Article 30

5.3 Data Protection agreements with Personal Data Recipients

On an ongoing basis, the PSA puts in place appropriate contracts / memoranda of understanding / bilateral agreements with third parties with which personal data is

shared. This includes state agencies and other government departments. The agreements specify the purpose of sharing the data, the requirements for security of the data and the requirements for termination of the agreement and the return / deletion of the data shared.

All such agreements are in accordance with the relevant statutory provisions of each body.

5.4 Data Protection by design and default

In accordance with Article 25 of the GDPR, the PSA implements technical and organisational measures to give effect to the principles of the protection of personal data and to ensure that, by default, only personal data necessary for each specific purpose of the processing are processed. Such measures include the development of organisational policies and procedures such as Acceptable Usage Policy and Digital Communications Policy and the implementation of security measures to secure the data.

5.5 Data Protection Impact Assessment (DPIA)

Where the PSA considers that proposed processing (in particular processing that involves new technology), poses a high risk to the rights and freedoms of the data subjects involved, the PSA will carry out a DPIA. The PSA's Data Protection Officer will be consulted in relation to each DPIA completed. Where technical and/or organisational measures proposed will not mitigate the high risks previously identified, the Data Protection Commission will be consulted as appropriate.

5.6 Transfer of personal data outside of the European Union

The PSA does not currently transfer any personal data outside of the European Union and has no plans to do so. If in the future this changes, the PSA will ensure that, prior to transferring any personal data outside of the European Union, appropriate safeguards are in place.

5.7 Personal data breaches

The GDPR defines a personal data breach as meaning

'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

All staff in the PSA will notify the PSA's Data Protection Officer where they identify or suspect a breach of personal data. In accordance with GDPR, the DPO will notify the

Data Protection Commission without undue delay where a breach is likely to result in a risk to the rights and freedoms of the data subject(s) involved. The DPO will also assess if the breach is likely to result in a high risk to the data subject(s) involved. Where a high risk is identified, the DPO will arrange for the data subjects to be notified.

5.8 Personal Data Governance

Compliance with the GDPR is a key requirement for the PSA. The PSA's compliance framework will detail the arrangements in place to oversee, monitor and ensure compliance with data protection legislation.

5.9 Data Protection Officer

In compliance with GDPR Article 37.1(a) of GDPR, the PSA has a designated Data Protection Officer (DPO). In accordance with Article 38, the PSA will involve the DPO in a timely manner in all issues which relate to the protection of personal data and will support the DPO in performing the tasks referred to in Article 39 *Tasks of the Data Protection Officer*. The tasks assigned to the PSA Protection Officer in Article 39 include the following;

- Informing and advising the PSA and staff who process personal data, of their obligations under data protection legislation;
- Monitoring compliance with the GDPR and the Data Protection Act 2018 and the policies of the PSA in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff and the related audits.
- Providing advice where requested as regards the data protection impact assessment and monitoring its performance
- Cooperating with the Data Protection Commission
- Acting as a contact point for the Data Protection Commission on issues relating to processing and prior consultation.

6.1 Data Protection Contacts

Data Protection Officer
Mr. Keith Nolan
The Private Security Authority
Davis Street
Tipperary Town
Co. Tipperary
E34 PY91

Phone: 062 32615
Email: info@psa.gov.ie

Office of the Data Protection Commissioner
21 Fitzwilliam Square South
Dublin 2.
D02 RD28

Phone: 0761 104 800
Email: info@dataprotection.ie

APPENDIX A

Key definitions used in Data Protection legislation

Below are definitions of the key terminology used in the GDPR.

Personal Data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Subject is an individual whose personal data is processed.

Processing means any operation or set of operations which is performed on personal data, by manual or 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.

Special categories of data means any data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processor means a person, public authority, agency or other body who processes personal data on behalf of the controller.

APPENDIX B

Table 1 - Functions of the Private Security Authority Include
Granting of licences to individuals and contractors providing security services
Monitoring the provision of security services
Specifying standards and qualifications to be observed in the provision of security services.
Creation and Maintenance of Public Register of Licensees

Table 2 – Private Security Authority - Public Interest Tasks
Communication with Citizens
Communication with Members of the Oireachtas
Internal Government Communications
Administration of Official Duties