An tÚdarás Slándála Príobháidí
The Private Security Authority

Private Security Authority

(PSA)

Data Protection Policy

October 2024

Table of Contents

Document Control

Version:	V1.0
Prepared By:	Keith Nolan (Data Protection Officer)
Approved By:	Joe Duggan (Head of Corporate Affairs) Paul Scallan (Chief Executive)
Date:	31 October 2019

Version:	V2.0
Prepared By:	Keith Nolan (Data Protection Officer)
Approved By:	Dan Liddy (Head of Corporate Affairs) Paul Scallan (Chief Executive)
Date:	8 May 2023

Version:	V3.0
Prepared By:	Paul Chappell (Data Protection Officer)
Approved By:	Keith Nolan (Head of Corporate Affairs) John Phelan (Chief Executive)
Date:	23 October 2024

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 licenses 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
    - Enforcement Guard
- 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 functions of the PSA are outlined in Appendix B.

2. Purpose

The PSA necessarily collects, processes and stores personal data from our licensees, staff, service providers and others to meets its obligations under the Private Security Services Act 2004 (as amended). Its goal is to ensure that data is retained in a way that is in accordance with the EU General Data Protection Regulation, 2016/679 (GDPR) and the Data Protection Act 2018. In accordance with 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. The key definitions used in the GDPR are set out in Appendix A.

3. Law Enforcement Directive

The Law Enforcement Directive, or 'LED', is a piece of EU legislation, parallel to the GDPR, which also has effect from May 2018. As suggested by its name, the LED deals with the processing of personal data by data controllers for 'law enforcement purposes' – which falls outside of the scope of the GDPR.

The LED is a Directive rather than a Regulation, and this requires transposition into Irish domestic law to take effect. This transposition is achieved through the Data Protection Act 2018 ('the Act'), primarily through 'Part 5 – Processing of Personal Data for Law Enforcement Purposes'. The PSA is a 'competent authority' for the purposes of LED and processing is done for 'law enforcement purposes' by the C&I Division.

Under the Private Security Services Act 2004, the PSA has specific powers that provide the legal basis for its data processing activities under the LED.

- Section 8 – Functions
- Section 13 – Investigations by Authority
- Section 14 – Inspectors
- Section 15 – Power of entry and inspection
- Section 21 38 – License to Provide Security Services
- Section 39 – Investigation of Complaints

The Data Protection Principles of the Law Enforcement Directive (LED) place specific obligations on the Private Security Authority (PSA) for the processing of personal data in the context of its regulatory and enforcement functions within the security industry. The PSA are committed to ensuring all provisions are implemented in relation to data processing for law enforcement and prosecution purposes.

4. 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.

5. Data Protection Principles

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

- Processed in a way that is lawful, fair and transparent;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and is limited to what is necessary;
- Accurate and kept up to date;
- 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
- Processed in a manner that ensures appropriate security of the data.

6. Application of Data Protection Principles in the PSA

Article 5(2) of the GDPR also obliges the PSA to "*be responsible for, and be able to demonstrate, compliance with the principles*". The PSA's policies and procedures are designed to ensure compliance with these principles.

6.1 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.

6.2 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)

6.3 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.

6.4 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.

6.5 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.

6.6 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 will undertake training in relation to their personal responsibilities for the protection of personal data.

7. 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.

7.1 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.

7.2 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.

7.3 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.

7.4 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.

7.5 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.

7.6 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.

7.7 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.

7.8 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.

8.0 Responsibilities of the Private Security Authority

The PSA is responsible for the following:

8.1 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.

8.2 Maintaining a record of data processing activities

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

8.3 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 must be in accordance with the relevant statutory provisions of each body.

8.4 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.

8.5 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.

8.6 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.

8.7 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'***.

A clear assessment procedure and Standard Operating Procedure (SOP) for data breaches is to be implemented. All staff in the PSA will notify the PSA's Data Protection Officer (Paul Chappell) and the PSA Data Officer (Keith Nolan) where they identify or suspect a breach of personal data. A detailed SOP for handling data breaches will be circulated annually by the Data Protection Officer. 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 be the point of contact for the Office of the Data Protection Commissioner (DPC) and submit any required report to the Office of the DPC. Where a high risk is identified, the DPO will arrange for the data subjects to be notified. The Data Breach and Data Incident Handling Standard Operating Procedures (SOP) for the PSA can be found in APPENDIX C.

8.8 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.

8.9 Employee Responsibility

PSA Employees play a crucial role in ensuring that the PSA collects, processes and stores personal data from our licensees, staff, service providers and others to meets its obligations under the Private Security Services Act 2004 (as amended). Staff are obligated to ensure that PSA's policies and procedures are implemented correctly to ensure compliance with these principles. PSA staff will undertake training in relation to their personal responsibilities for the protection of personal data.

8.10 Data Protection Roles

The 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.

The Data Officer

The Data Officer (DO) will play a key role in improving the management of data within the PSA. They will work with key stakeholders and decision makers within the PSA to identify how the Data Sharing and Governance Act can be implemented effectively. As such, the DO will coordinate and prepare Data Sharing Agreements by engaging with all internal contributors to assess the need for data sharing and provide support for the sharing and governance of that data.

It's important to note that the DO role is distinct from the Data Protection Officer (DPO) role in an organisation. The DPO is still responsible for ensuring that data is compliant with Data Protection law and consistent with GDPR. The Data Officer should be someone who will act as a champion for data-sharing in their organisation, offering an insight into to the data sharing practices and projects in their organisation and sharing updates on related work. The DO will play a key role in the new process for sharing data. It is also envisaged that the DO will:

- Identify opportunities within the organisation for data sharing under the Act and work with the DGU on any matters or queries in relation to the Act.
- Promote the sharing of data, and improved data management and practices within their organisation.
- Act as a single point of contact between their organisation and the DGU. This will allow us to ensure full and open communication on initiatives being undertaken by the DGU. It will also allow you to keep the DGU up to date with data-sharing progress in your organisation. The DGU will keep you fully informed about developments in the area of Data Strategy, Data Policy, Data Analytics and the work of the Data Governance Board.

It should be noted that the Data Officer role is a different responsibility from the Data Protection Officer role in that the first is responsible for advocating and seeking opportunities to share data and the second is responsible for ensuring all data sharing is compliant with GDPR and all relevant legislation. Consequently it is important that these roles should NOT be filled by the same person.

9. Data Protection Contacts

Data Protection Officer
Mr. Paul Chappell
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 Commission
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

GDPR refers to the EU General Data Protection Regulation, 2016/679 (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.

DPIA means Data Processing Impact Assessment. A template DPIA must be completed in any circumstance where a Private Security Authority (PSA) business unit proposes to process personal data. Article 35 prescribes that a Data Protection Impact Assessment (DPIA) shall be conducted by a Data Controller where a type of data processing (in particular using new technologies) is likely to result in a high risk to the rights and freedoms of individuals. Article 35(3) sets out a number of specific instances in which Data Controllers must conduct a DPIA. Similarly, Section 84 of the Data Protection Act requires a DPIA for Law Enforcement Data (LED).

DPO means Data Protection Officer (Paul Chappell)

Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

Private Security Services Act refers to the Private Security Services Act 2004 (as amended).

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. (i.e. PSA is a data controller)

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

APPENDIX C

Data Breach and Data Incident Handling Stand Operating Procedure (SOP) for the PSA

Introduction

Breaches of information security/confidentiality could potentially compromise business operations and be damaging to the Private Security Authority (PSA) as a whole. Such breaches could also pose a threat to the personal safety or privacy of an individual(s). It should be noted that the PSA treat data breaches very seriously and any employee who becomes aware of a likely data breach and fails to notify the relevant officer, or any negligent or malicious action by an employee resulting in a data breach may be subject to the PSA's disciplinary procedure depending on the severity of the breach. Examples (not exhaustive) of these types of incidents include:

- Emails been sent to the wrong person
- Damage to or theft/loss of personal information (either manual or electronic);
- Leaving personal information/records in a public area;
- Incorrect disposal of personal information where no longer required;
- Unauthorised access to personal information;
- Unauthorised disclosure of personal information in any format including verbally;
- Transfer of personal information to the wrong person (by email, fax, post, or phone);
- Sharing of computer IDs and passwords.
- Phishing and malware attacks on the IT system

While this document focus on what a staff member should do in the event of a Data Incident or Data Breach, the following procedures would also be applicable to Data Processors.

Procedures to be followed if a Breach or Data Incident occurs or is suspected

Every breach must be taken seriously and reported according to the process as follows. If there is any doubt about what constitutes a breach or a data incident, staff should contact the Data Protection officer (DPO) or a member of the senior management team.

IT related data Incidents

If the Breach involves a mailbot (emails being sent without you clicking "send") or suspicious activity on your screen, disconnect your computer from the network and turn off the machine.

If this or any other breach is **IT related**, immediately contact Paul Chappell (the DPO) who will contact the IT helpdesk so that containment measures can be deployed.
IT Support Contact No. 01 602 8888
Email: helpdesk@justice.ie

Then contact the DPO ASAP.

DPO Contact No. 087 4946792
Email: PChappell@psa-gov.ie

Once this is done the following steps should be implemented.

First Steps (usually the staff member)

1. Where a member of staff suspects that a breach has occurred (including "Outside of Working Hours", or has been informed that a breach has occurred, they must report this immediately to their Line Manager **and** to the DPO.
2. The reporting staff member and/or line manager to fill in the relevant portions of the Breach Report Form (see below)

Containment and Reporting Assessment of a Breach/Data Incidents

1. The DPO will:
    a. Implement immediate containment measures if possible
    b. Record the incident in the Breach log
    c. With The Data Officer (Keith Nolan), undertake an assessment of risks (including a breach reporting assessment) involved in the incident in terms of the potential adverse consequences for individuals and how likely these are to happen
2. Following these assessments and in consultation between the CE, DPO and Data Officer, it will be determined:
    a. Whether further containment action can be implemented
    b. Whether additional investigation is warranted
    c. Who needs to be notified of the breach.
        i. If the breach poses a Risk to the Data Subjects involved, the Data Protection Commission will be informed within 72 hours of first becoming aware of the breach
        ii. If the breach poses a high Risk to the Data Subjects involved, the Data Protection Commission will be informed within 72 hours of first becoming aware of the breach as will the Data Subjects involved (if it is possible to do so
        iii. If appropriate other bodies may be consulted / briefed such as An Garda Siochána and the Depart of Justice.
3. The Data Protection Officer will be the point of contact for the Office of the Data Protection Commissioner and submit any required report to the Office of the Data Protection Commission.

Further investigation and Preventative measures

4. Where it is determined, based on the Risk assessment, that the data breach represents a high risk to the data subject or to a significant number of data subjects in circumstances where the data is extremely sensitive or where there is significant media interest in the breach, the Chief Executive will

convene a meeting with the Data Officer and the DPO to review actions taken and to agree on the next steps in the process.

5. Where appropriate, the DPO or nominee will lead an investigation to establish the circumstances of the incident, the extent of any loss and the implications for the organisation, which may involve interviewing staff or third parties involved. Such a report will include preventative measures that should be implemented to ensure that a similar incidence does not reoccur.

6. The DPO will take action to ensure that lessons learned from the incident are applied to existing policies and practices. This may include implementing changes to or introducing additional systems of control, increasing awareness of information risk, or disseminating lessons learnt.

Breaches "Out of Hours"

It is noted that data breaches which require a PSA response may first come to light in the media. It is therefore critical that the PSA has in place an 'out of hours' system to manage and respond to data breaches. Therefore, the following steps will be applied if such a breach occurs:

- Outside of normal working hours (e.g. weekends, bank holidays, etc.) the Data Protection Officer (DPO) is responsible for managing 'out of hours' breach reporting.

- To report a personal data breach incident outside of normal working hours, contact can be made to the PSA Data Protection Officer (DPO) Paul Chappell (contact: 087-494-6752), who will in turn contact the Data Officer (Keith Nolan) and Chief Executive (John Phelan).

THE PRIVATE SECURITY AUITHORITY - HIGHLY CONFIDENTIAL

FORM FOR REPORTING A SUSPECTED INFORMATION SECURITY / DATA BREACH			
FIRST INSTANCE RESPONSE			
Your Name:		Division:	
Today's Date:	Tel No:	E-mail Address:	
Date of Incident:		Time of Incident:	
Brief Description of Incident: (include possible impacted data subjects etc...)			
To your knowledge was any of the following involved? Telephone ☐ Theft ☐ Fax ☐ Fraud ☐ Photocopier ☐ Unauthorised Access ☐ Computer Hardware ☐ Customers ☐ E-mail ☐ Third Parties ☐ Internet download ☐ Copyright ☐ Virus ☐ Other (specify below) ☐			
Was any Internal or Confidential information compromised?		Y ☐	N ☐
Who Was Notified:		Time of Notification:	
DPO / MANAGERS RESPONSE			
Your Name:		Position:	
Today's Date:	Tel No:	E-mail Address:	
Brief Description of Any clarification/investigation undertaken / Determination of whether a breach has occurred:		**Containment Actions:** For example: • Immediately contain the breach by: ○ stopping the unauthorized practice ○ recovering the records ○ shutting down the system that was breached • Correcting weaknesses in physical security. • Contact your DPO or the person responsible for privacy and security in your organization. • Notify the Guards if the breach involves theft or other criminal activity)	
Evaluate the risks associated with the Breach (Eg. Personal Information Involved; Cause and Extent of the Breach; Individuals Affected by the Breach; Foreseeable Harm From the Breach)		**Determining who requires to be Notified:**	
Preventative measure :			

An tÚdarás Slándála Príobháidí
The Private Security Authority

Private Security Authority
Davis Street Tipperary Town Co. Tipperary E34 PY91
T: 062-32600
E: info@psa-gov.ie W: www.psa-gov.ie