An Coimisinéir Cosanta Sonraí / Data Protection Commissioner

An Garda Síochána:

Final Report of Audit

Issued March 2014

Executive Summary

The Office of the Data Protection Commissioner (ODPC) carried out an audit of data protection in An Garda Síochána (AGS) over the years 2011 to October 2013. The audit consisted of an examination of documentation provided by AGS, discussions with AGS senior management and on-site inspections at AGS HQ in Dublin, the AGS Vetting Unit in Thurles, the AGS Information Services Centre (GISC) in Castlebar and Garda stations in Donnybrook, Mullingar and Limerick.

The audit was carried out by reference to the requirements of the Data Protection Acts and the elaboration of those requirements contained in the ODPC-approved Data Protection Code of Practice for AGS. Full cooperation was received from AGS, including access to all relevant documents, systems and individuals.

A central focus of the audit was the main IT system used by AGS for recording data, PULSE. This investigation involved detailed examination of the recording of data by GISC and by individual AGS members, the classification of such data and the systems in use to maintain the accuracy and security of the data and to prevent improper disclosure. The audit report describes in detail the procedures in place with regard to how certain personal data or episodes in an individual's dealings with AGS are recorded. Often, as evidenced during the audit, this entails the management by AGS of large unstructured formats of data. In our findings, we highlighted areas where improvements are required but equally we acknowledged practices and procedures where there were no data protection issues arising. Overall, we found the majority of the areas examined demonstrated a professional police force operating in compliance with data protection legislation.

While the audit team was generally satisfied with the in-built data protection mechanisms in PULSE, this was not the case in relation to the oversight of access by individual AGS members to records of individuals and the related risk of disclosure outside of AGS. The Team came across disturbing instances of such improper access and found that scheduled audits of accesses to PULSE, as provided for in the AGS Data Protection Code of Practice, had not been carried out. However, implementation of that aspect of the Code had commenced by the time the audit ended. In addition, as a response to the inappropriate access detected during the audit, AGS instigated a three-pronged approach to counter any future inappropriate access namely HQ Directive 95/2012, a revised warning notice on PULSE displayed to all users as they log on and a programme of random audits conducted by the Garda Professional Standards Unit. We expect An Garda Síochána to now actively enforce the terms of HQ Directive 95/2012 and take strong and appropriate disciplinary action against any persons abusing their access to PULSE and prosecutions against any person found to be using such access for gain.

The Team examined the processes in use to respond to requests from employing organisations for vetting of employees and requests from individuals for access to their personal data. We consider that a fundamental area requiring clarification by AGS to data subjects is to outline clearly what will be disclosed back by AGS via an authorised signatory to an organisation for vetting purposes as opposed to what a data subject can expect to receive via a subject access request made to AGS under section 4 of the Data Protection Acts. This is the source of frequent enquiry to this Office when a data subject or their solicitor makes an access request to AGS and views the content supplied in response by AGS. Both processes rely heavily on the accuracy of data contained in PULSE and the Team was satisfied that both processes were subject to appropriate procedures, notably as regards data accuracy.

The audit included an examination of the processing of personal data in relation to the arrest and detention of individuals. Such processing is significantly determined by detailed statutory requirements, including those related to the taking of fingerprints and photographs. Failure to comply with such statutory requirements can result in difficulty in securing convictions in Court. The Team did not come across any significant issues in this area.

An area of concern is the use for criminal investigation purposes of fingerprints of individuals required to provide such fingerprints in connection with applications for asylum, visas and residence. We indicated to AGS that we consider some practices in this regard raise issues from a data protection perspective and recommended that AGS revisit this issue with the Attorney General in the interests of clarity for all parties concerned taking account of the European legislative context.

The Team examined the processes in use for AGS access to subscriber data held by telecommunications companies and there were no data protection issues of concern arising in this regard.

The Team examined the use of CCTV by AGS as well as the AGS Automatic Number Plate Recognition (ANPR) system. There were some minor recommendations with regard to CCTV but no data protection issues of concern arising in regard to ANPR.

.

Other areas examined included the processing of data in relation to sex-offenders; AGS access to vehicle and driver information; data disclosures to 3rd parties; and exchange of data with other countries.

In the course of the various inspections, the Team noted that AGS had not yet developed a comprehensive policy on data retention – one of the commitments contained in the Code of Practice. AGS committed to examining the organisational implications of the retention or deletion of all categories of personal data held by AGS.

Though not specifically raised in the course of the audit, it is the view of ODPC that AGS should have a dedicated data protection unit, headed by an Officer with direct access to the Garda Commissioner.

A number of detailed recommendations were made to AGS arising from the audit. These are listed below, together with the responses of AGS.

Recommendations

- In terms of monitoring access by members of AGS to PULSE on a proactive basis, the audit tool described at paragraph 4.8 should be implemented immediately thereby enabling samples of logs to be checked at a local level on a routine basis in order to check for any unusual access patterns. When introduced, these new monitoring measures should be made known to staff to deter inappropriate access. In addition, it is considered that any inappropriate accesses discovered as a result of the introduction of this audit tool should be dealt under AGS disciplinary procedures.

  [Since the inspection took place AGS informed this Office that the Garda Professional Standards Unit in accordance with its remit under the Garda Síochána Data Protection Code of Practice and HQ Directive

95/2012 has commenced random audits of the completion of the Item of Inquiry dialogue box in respect of Persons, Vehicles, and Location inquires. HQ Directive 95/2012, HQ Directive 14/200I and Garda Code 32.15(3) requires that information recorded in the 'Item Inquiry Details' dialogue box is as 'informative as possible' and should be sufficient to ensure that subsequent enquiries obtain maximum benefit from the system '.

Where the information recorded in the 'Item of Inquiry Details' dialogue box is insufficient to demonstrate compliance with requirements of the Data Protection Acts, An Garda Síochána Data Protection Code of Practice and the requirements of HQ Directive 95/2012, HQ Directive 14/2001 and Garda Code 32.15(3) the following is required;

- *Completion of 'Actions Taken' column with details of the measures taken to address the information deficit. The 'Actions Taken' column is part of a spreadsheet populated with enquiries where members have provided a deficit of information.*
- *Details on how quality of information provided by members of a District in the Item of Interest's dialogue box is monitored?*
- *Details on any system/process which is in place to monitor the quality of information provided in the Item of Interest's dialogue box?*
- *Action taken as a result of the Audit to increase the level of compliance in the completion of Item of Interest's Dialogue box by District staff?*

Of the 48 Districts that have been audited to date, the 'Follow-up' audit has commenced in 12 of these Districts.

The Garda Professional Standards Unit are currently working with IT Section to develop an "Item of Interest Report" for District Officers where they can view checks carried out by members of their District Force and in particular the reasons being recorded on the PULSE system for these checks. This report was deployed in August 2013 is currently being piloted by the Garda Professional Standards Unit.

AGS confirmed to the Team that the revised audit tool would allow a reviewer to check on all previous activity of a user if it was deemed necessary to query this. The review system places a responsibility on District Superintendents to require members to account for the business reason for a specified percentage of accesses to the system per month. These accesses are chosen at random by the review system and provided to the Superintendent in each case. AGS confirmed that the conduct of the review will be a performance requirement of each Superintendent with failure to do so leading to action.]

- Section 2(1)(c) of the Data Protection Acts 1988 and 2003 provides that a data controller shall not retain personal data longer than is necessary for the purpose or purposes it was obtained. In determining appropriate retention periods for personal information, data controllers must have due regard for any statutory obligations. If the purpose for which the information was obtained has ceased and the personal information is not required for ongoing policing purposes, the data must be deleted or disposed of in a secure manner. In various sections throughout the report, the issue of the retention of certain types of data and records within AGS is examined. Overall, it is recommended that AGS examine the organisational implications of the

[AGS stated they are guided by the Criminal Procedure Act 1993, the National Archives Act 1986 and the Data Protection Acts 1998/2003 in relation to the retention and destruction of records in An Garda Síochána]

In particular, AGS policy with regard to the retention of certain categories of intelligence should be examined by AGS in conjunction with the ODPC.

[Since the inspection took place AGS stated that the above recommendation has been forwarded to Security and Intelligence for their consideration. At a generic level PULSE functionality has been developed which allows intelligence records to be categorised. However AGS operates strictly with the context of the legislative framework of the proposed acts – National Vetting Bureau (Children & Vulnerable Adults) Act 2012 and Criminal Justice (Spent Convictions) Bill 2012.]

- The integration of the fingerprints of asylum, visa and residence applicants with fingerprints taken for criminal investigation purposes raises issues from a data protection perspective.

  [In response AGS stated that the decision to search the entire AFIS database including GNIB, eVisa, asylum and Interpol fingerprints for criminal investigation purposes is necessary. This is in accordance with specific advice received from the Attorney General in relation to this matter.]

  It is recommended that AGS revisit this issue with the Attorney General in the interests of clarity for all parties concerned taking account of the European legislative context.

- The right of application to delete fingerprints held on AFIS should be added to the written consent form signed by a person who voluntarily provides finger prints and also to any written information provided to a person who is being compelled by AGS to be fingerprinted. All information provided to data subjects regarding retention periods for fingerprints and associated rights of deletion must be reviewed and amended upon the enactment and commencement of the "Criminal Justice (Forensic Evidence and DNA Database System) Bill, 2013".

  [In response AGS stated that this recommendation will be considered following the enactment of the forthcoming "Criminal Justice (Forensic Evidence and DNA Database System) Bill, 2013".].

- It is recommended that the Criminal Records Information Systems Bill 2013 which is currently at draft stage in the Oireachtas is passed as soon as possible in order to underpin the legal basis for the operation of ECRIS.

- A policy framework and guidance should be drawn up outlining the circumstances in which all disclosures for vetting purposes will be made under forthcoming legislation with a clear framework outlining the range of what may be disclosed and in what circumstances and the exact time period under which non-convictions and old or minor convictions may become 'spent'.

[AGS in response indicated that this recommendation will be considered following the enactment of forthcoming legislation.]

- A records management programme should be put in place to systematically review and check the accuracy of PULSE records on a rolling basis. This is essential to ensure that the categorisation of individuals and incidents on PULSE reflects the most current status in relation to the incident recorded.

  [Since the inspection took place AGS informed the Team that Reporting Services at the IT Section deployed the 'Incidents with Incomplete Proceedings Report' in 2009. This report was designed to assist in the management of an incident's lifecycle, in particular in relation to incidents with a 'Suspected Offender'. An additional report has been developed to monitor the lifecycle in relation to incidents of a sexual nature. A request has been made to the IT Section to extend these enhancements to the existing 'Incidents with Incomplete Proceedings Report'. A number of additional reports and further enhancements have been requested to assist in the management of all incident lifecycles on PULSE. HQ Directive 64/2013 and 79/2013 now also apply in this regard.]

- Generic forms for fingerprinting, palm prints and photographs should be designed, signed off and circulated for universal use to ensure consistency.

  [AGS advised ODPC that in December 2012, a revised PC-02 form (which deals with photographs) was added to the list of forms that are available on AGS portal. The primary purpose of the PC-02 form is to have the photograph uploaded onto PULSE. This form records the person and photograph details, the authority for the taking of the photograph (includes voluntary photographs), the officer that authorised the uploading of the photograph onto PULSE and the details of the CIO that added the photograph details onto PULSE.

  A revised form has been developed, which notifies a person that there is a legal requirement for the taking of their fingerprints / palm prints under Section 28 of the Criminal Justice Act, 1984. A revised form has also been developed which records the consent of a person for the taking of their fingerprints / palm prints.]

- All requests for call and internet traffic data are to be authorised by the Chief Superintendent on a case by case basis rather than on an aggregate basis at the end of a particular time period.

  [AGS confirmed to the Team that every application is currently considered on a case by case basis by the Chief Superintendent.]

- PCs should be locked down against USB access by default and access by a USB drive should only be allowed on a case by case business need.

  [Since the inspection took place AGs informed the Team that IT Operations have conducted a review of the usage of USB drives and has recommended the lockdown of all clients USB ports to only allow access by Garda issued encrypted external drives. This will need to be co-ordinated with the migration of all Garda clients to provide secure file storage to all Garda members.

When the migration of all users is completed the requirement for USB drives will be considered as part of a wider review of ICT Security.]

- Accounts set up for student Gardaí who do not graduate should be deleted rather than disabled.
  [AGS response: the policy of AGS is to disable accounts for all users on retirement, resignation etc. Students do not have access to 'live' PULSE and they are only granted access when they are attested.]

- A PULSE incident number should be recorded in respect of each download from Garda CCTV footage.
  [AGS informed the Team that all matters pertaining to Garda CCTV policy are currently under review].

- Requests for downloads of CCTV footage made by AGS to third parties should be followed up in writing at all times.

  [AGS stated that it submits a request in writing for CCTV when requested by the third party. Currently there are specific arrangements in place when requesting CCTV from Financial Institutions. AGS comply with other requests in line with the third parties policies.]

- AGS should review its policy for handling requests for access to AGS CCTV footage made under Section 4 of the Acts.

  [Since the inspection took place AGS indicated that it will process requests for AGS CCTV received under a Section 4 Data Protection Act access request. Current policy indicates that "Video recordings will be used for Garda investigative purposes only and on no account will they be released to outside bodies or individuals for private or civil use except where such has been ordered through the normal judicial process".]

- A manual audit trail should be put in place for all CCTV downloaded from Garda CCTV systems.

  [AGS's current Code of Practice in relation to the downloading of CCTV outlines the following instructions: Code of Practice 6.2 - The review facility at each respective location shall be accessed only by Garda members authorised by the local District Officer to make use of that facility for the purpose of reviewing video material recorded on that or another similar system. Any member making use of the review facility must complete an entry in official documentation, which will also include the Superintendent's authority.]

- In line with Section 4.1(i), all staff performing duty in the CCTV monitoring area should enter in the CCTV Incident Log Book details of the time and date of commencement and completion of such duty

  [*AGS stated that it is operating in compliance with section 4.1(i) of the Code of Practice for CCTV in Public Places in relation to staff performing duty in CCTV monitoring areas*.]

- It is recommended that the AGS Vetting Unit be adequately resourced to deal with data subject access requests. As an organisation, AGS needs to instil

within each garda district a culture of compliance with the 40 day statutory requirement in terms of processing of access requests to ensure AGS can meet the 40 day deadline under which it is bound to respond to an access request.

[AGS stated that this recommendation is receiving ongoing attention]

- A dedicated Data Protection Unit should be established within AGS, headed by an officer with a direct reporting relationship to the Garda Commissioner.
- It is recommended that AGS engage further with the ODPC on the use of GPS co-ordinates when plans for their deployment are at proposal stage.
- The ODPC recommends that all court outcomes are fed through to PULSE electronically via CJIP so as to ensure the accuracy of information held on PULSE.
- It is recommended that all access requests made by former or serving members are processed in a dedicated queue separately within AGS.

1. Background and Legal Basis for Inspection

On 03 March 2011, the Data Protection Commissioner (DPC) wrote to the Assistant Commissioner of An Garda Síochána (AGS) to indicate that a data protection audit of An Garda Síochána would commence during 2012

Section 10(1A) of the Data Protection Acts 1988 & 2003 states that

> *"The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and to identify any contravention thereof".*

Under this authority the Commissioner instructed that an inspection of An Garda Síochána be conducted so that he would be in a position to assure the public that their personal data held by the Gardaí is handled in line with the requirements of the Data Protection Acts. The Office had concerns that it was not in a position to provide that assurance despite the provisions of a Code of Practice agreed between An Garda Síochána and the Office in 2007. That Code recognised that the Data Protection Acts provide a clear basis for AGS to process personal data in relation to the investigation, prevention and detection of crime and that there is an exemption from aspects of the law where personal data continues to be processed for that purpose.

From the outset of discussions on the conduct of the audit, full co-operation was received from AGS. This continued during the on-site inspection phase of the audit where AGS adopted an approach of full transparency and openness with the Office with a view to identifying any issues where improvement was necessary and remedying any such areas. This approach was reflected in the action taken by AGS in the course of the audit in response to points raised by the Audit Team.

2. PRE-INSPECTION

The Office of the Data Protection Commissioner (hereafter referred to as ODPC) met with An Garda Síochána at Garda HQ, Phoenix Park on Wednesday 31 August 2011 to discuss plans to audit AGS in more detail. The two organisations met again in November 2011 and AGS provided the ODPC with comprehensive progress updates concerning information management and data governance projects ongoing in AGS. This was followed by a meeting in April 2012 where it was agreed the audit would commence as soon audit resources within the ODPC became available.

Following on from all previous communications, the ODPC wrote to An Garda Síochána on 23 October 2012 giving notice of the dates on which it intended to conduct an initial inspection (7-8 November 2012) with a pre-audit meeting setting out the agenda and scope scheduled to take place on November 5th 2012. An Inspection Team was selected, consisting of Gary Davis, Deputy Commissioner, Eunice Delaney, Assistant Commissioner and Paula Nerney, Senior Compliance Officer.

The purpose of the audit was described as being

> *To ascertain if the procedures and practices employed by An Garda Síochána are in compliance with the provisions of the Data Protection Acts, 1988 and 2003*

The ODPC indicated to the Commissioner of An Garda Síochána that the approach would be to track and examine the movement and management of personal data throughout the organisation of An Garda Síochána and to identify any necessary measures to deal with deficiencies regarding the handling of personal data. The scope of the audit was acknowledged in advance by both parties as vast in terms of the datasets maintained by AGS. In view of this, it was agreed to refine and identify particular areas for examination such as the recording of incidents and crimes on PULSE, possible inappropriate access to PULSE by members of AGS, the taking and use of fingerprints and also to examine specific areas administered by AGS such as CCTV and Garda vetting.

The Office indicated that it planned to focus initially on the following areas:

- Circumstances under which information is entered onto PULSE[1]
- Guidelines/Manuals available to members of AGS providing clarity on use of PULSE and data entry
- Data Quality/Accuracy of data held on PULSE e.g. recording of victims/suspects/witnesses
- Circumstances under which members of AGS may access PULSE
- Procedures and systems for checking Garda access to PULSE e.g. Exceptional Activity Reports, random spot checks
- Access requests by data subjects to data held about them on PULSE (dealt with by Garda Vetting Unit, Thurles)
- Notice of court outcomes/sentences and recording of these on PULSE
- NVDF[2] data on PULSE (including penalty points)
- Speeding and speed monitoring vans - data processing on behalf of AGS
- Firearms Data - connection to PULSE
- Capture and storage of personal photographs
- Fingerprints & Automated Fingerprinting Information System (AFIS)
- Garda Information Services Centre (Castlebar)

It was signalled to AGS that it was the intention of the Audit Team to select other areas within AGS for examination as the audit progressed and more detailed schedules would be agreed on foot of the preliminary meeting. ODPC also indicated it intended referring to the detailed AGS registration with the ODPC to assist the Team in the planning and audit process itself.

In addition to visits to Garda HQ Garda stations across the country (Limerick, Mullingar and Donnybrook were randomly selected for examination), the Team conducted inspections of the Garda Vetting Unit in Thurles and the Garda Information Services Centre (G.I.S.C) in Castlebar.

[1] Police Using Leading Systems Effectively – AGS central IT system
[2] National Vehicle Driver File

3. OVERVIEW OF AN GARDA SIOCHANA

The Garda Commissioner is responsible for the general direction, management and control of An Garda Síochána. The Commissioner is appointed by the Government. While the Minister for Justice, Equality & Law Reform is responsible to the Government for the performance of An Garda Síochána, it is the Commissioner who is responsible for the operational aspects of the organisation on a day to day basis.

An Garda Síochána's core functions include:

- the detection and prevention of crime;
- ensuring the nation's security;
- reducing the incidence of fatal and serious injuries on our roads and improving road safety;
- working with communities to prevent anti-social behaviour;
- promoting an inter-agency approach to problem solving and improving the overall quality of life.

The Garda Commissioner's Management Team is comprised of: a Deputy Commissioner in charge of Operations; a Deputy Commissioner in charge of Strategy & Change Management; Chief Administrative Officer (CAO); 8 Assistant Commissioners; Executive Director of Finance; Executive Director of Information and Communication Technology; Director of Communications and a Chief Medical Officer.

For policing purposes the country is divided into 6 regions, each of which is commanded by an Assistant Commissioner. The 6 regions are:

Dublin Metropolitan Region
Northern Region
Western Region
Eastern Region
Southern Region
South Eastern Region

Each region is divided into divisions commanded by a Chief Superintendent, and each division is then divided into districts commanded by a Superintendent. A Superintendent in charge of a district is also known as the District Officer. He/She is assisted by a number of Inspectors. The districts are divided into sub-districts, each normally the responsibility of a Sergeant.

4. PULSE

The PULSE system – the core Garda information platform - was a central focus of the audit. Compliance by AGS with the data protection principles of adequacy, accuracy, access and security is highly dependent on the architecture and use of PULSE. The Team therefore devoted significant time to understanding the PULSE system and identifying any weaknesses from a data protection perspective.

The accuracy of information on PULSE is a key issue from a Garda operational perspective but also from a data protection perspective as incorrect information in relation to an investigation or a court outcome can have devastating implications for

an individual. This can be particularly the case where a person is vetted. With the new statutory basis for vetting set to commence shortly, the accuracy of information on PULSE comes into even sharper focus. At present a person undergoing vetting consents to the disclosure of court outcomes. So called “soft information”, i.e. non court outcomes is not disclosed. The ODPC understands that the Vetting Act in its current form will provide that such information can be disclosed in certain circumstances subject to safeguards. As PULSE is the central source of all such information, this will increase the requirement for accuracy on PULSE. It will also require that increased attention is paid to non-conviction information on PULSE.

4.1 PULSE Overview

At the commencement of the audit the Team met with AGS Assistant Commissioner, Jack Nolan, Inspector John Jacob, Executive Director of ICT Liam Kidd, Principal Officer Aeneas Leane, Assistant Principal Kieran Downey and Superintendent Denis Ferry.

The Team was subsequently introduced to Garda and civilian staff with relevant responsibility for and experience of the areas under inspection during the course of the audit in Garda HQ and across a variety of locations around the country.

In terms of IT in AGS generally, AGS outlined that its Garda Information Systems Migration Project began several years ago and is still ongoing. A 2009 review of IT systems led to a new **HQ Directive on Information Security** (Directive 118/2009). AGS also referred to a new **Internet and Email Policy** issued in April 2012.

AGS stated that PULSE is essentially based on incidents and the workflow from an incident that may arise e.g. an assault, date of assault, suspect, injured party would be entered onto PULSE and a narrative signalled such as **'summons waiting to be served'** or a narrative chain such as **'incident'-'summons' - 'charge' - 'bail'**.

AGS further outlined that the current status of an incident is established based on the information recorded in the narrative of the incident in conjunction with information recorded within the incident. Information is also ascertained from the incident catalogue and its associated records. For example, the current status of an incident could be that a bench warrant was issued in court - this would be ascertained based on the warrant being linked to the court outcome which is linked to the charge sheet that was created from that incident for that particular person record.

AGS provided the Team with a comprehensive overview of PULSE from an operational and technical perspective, utilising the knowledge and expertise of their Chief Systems Architect who outlined how PULSE had been constructed and how it operated. This was supplemented with input from security specialists working within the Garda’s IT Division and a practical demonstration of how PULSE actually operates in practice from data entry to data searches and intelligence-gathering.

The Audit Team established that items such as statements made by individuals are kept manually in investigations files held in Garda stations and would not be available from PULSE but may or may not be referred to as part of an incident report on the system. Also, for documentation such as notes for the Director of Public Prosecutions (DPP) contained within an investigations file, AGS clarified that these were stand-alone and separate to data regarding the same incidents held on PULSE.

In terms of administration databases, An Garda Síochána use a correspondence tracking system for all correspondence within and outside the organisation – RECORD - which is not linked to PULSE. AGS clarified that there was an administrative filing reference tool on RECORD allowing stations within districts to access file numbers and thus request actual files. However, it is not possible to log into a district such as Killarney from another district and track a file. Where a file leaves a district, it is flagged on the system and the process of tracking the file commences again in the new district. AGS outlined to the Team that the transfer of files within and outside districts is done physically with no scanning of files or a central database from which to access files. AGS confirmed that the RECORD system is networked. There is however no central admin system in use throughout the force with members instead using local drives to create correspondence documents. From a data protection perspective such an approach creates a potential for correspondence and administrative records to remain on terminals at end of life but this is remediated by the Gardaí having a strong IT destruction policy and practice. In many respects, while the lack of a central admin system for creating and managing electronic records in a large data controller such as An Garda Síochána is perhaps surprising, account must be taken of the fact that the organisation is still very much manual records focused in terms of the conduct of investigations etc.

As an example, files sent to the DPP[3] are photocopied, with the original sent to the DPP and a copy file retained in the station, to which a copy of the DPP's instructions are appended, when received. A similar position pertains with files being transferred to the relevant state solicitor.

AGS acknowledged that whilst Pulse and Garda email systems are networked, there is no central document management system to deal with investigation files and all other routine correspondence. AGS stated it is their intention to network its entire system, however, current financial constraints essentially means this will not happen in the short term.

4.2 Demonstration of PULSE

During the course of the inspection in Garda HQ the Team were provided with two separate practical demonstrations of the live PULSE system, covering the interface itself, the various menus and options and the means by which the system could be interrogated.

Access to the live PULSE system was critical in order to allow the inspection team perform specific sample searches and views of PULSE in order to ascertain the type and extent of data held in particular fields and records.

4.3 Data Categorisation on PULSE[4]

The PULSE system is used to record incidents and intelligence reports. The system is designed to allow users to track accurately the incident from the original point of its recording through to details of the subsequent investigation such as court outcomes etc. Multiple incidents in relation to one person can be accessed by performing a

[3] Director of Public Prosecutions

[4] This issue was further examined in the context of the inspection of the AGS Vetting Unit – see Section 12

search on PULSE of that person allowing for a full picture of their interactions with the Gardaí. This is obviously important to assist in the investigation of crime but clearly from a data protection perspective there is also a requirement that all information recorded is accurate and up to date and only used for such purposes.

Incident Categories

AGS provided the Team with a list of the various categories of incidents which may be recorded on PULSE. The categories and the timeframes associated with recording these are as set out in Table 1.

Table 1

Incidents to Record	Within Tour of Duty	Within 24 Hours	Prior to Commencing Proceedings
Crimes	X		
Drug Offences	X		
Section 30 Arrests	X		
Searches – Sec 23 Misuse of Drugs Act 1977/84		X	
Public Order Act Offences (all)	X		
Domestic Violence Acts Offences	X		
Firearm Acts Offences	X		
Missing Persons	X		
Suspicious Death	X		
Sudden Deaths		X	
Property	X		
Traffic Accidents – Fatal or Personal Injury	X		
Traffic Accidents – Material Damage		X	
Drunk Driving Offences	X		
Dangerous Driving (involving arrest only) Offences	X		
UTs and Recovered Vehicles	X		
Section 41 Vehicles	X		
Summary Traffic Offences			X
Liquor Licensing Offences			X
Street Trading Offences			X
Other Miscellaneous Offences			X

Person Categories

Within the 'Person' category on PULSE, a person may be assigned the following range of Roles:

- Found Person (No longer available – Enhanced Missing Persons functionality)
- HSE Notification Concerning
- Injured Party
- Missing Person
- Questioned in relation to
- Reported by
- Searched
- Sought in connection with
- Suspect (Not available for selection in Non-Crime Incidents)
- Suspected Offender (Not available for selection in Non-Crime Incidents)

- Witness

AGS clarified that a person can have more than one 'role' in an incident. It is common for a person to have a role of 'Reported By' & 'Injured Party' within the same incident on PULSE. It is also possible for a person to have a role of 'Questioned in relation to' and to have an additional role of 'Suspect Offender' added at a later stage as the incident / investigation progresses.

As data categorisation is a significant data protection issue in terms of data accuracy, the Team explored issues related to certain of the incident categories and roles.

"Arrested"/"Detained"
The Team enquired as to whether there was a distinction between a person who is "arrested" or "detained" and AGS clarified to the TEAM that there is no difference. AGS outlined that it is Garda policy to ensure that where persons are arrested or detained in a Garda Station, a record is created and maintained on PULSE[5]. In cases where a person is detained in a public place (e.g. for the purpose of a search under the Misuse of Drugs Act) but not subsequently brought to a garda station it is also Garda policy to ensure that incident details are subsequently recorded on PULSE. During the course of the inspection in Mullingar, AGS Mullingar clarified that every physical search made of a person is recorded on PULSE.

"Suspected Offender"
The issue of the categorisation 'suspected offender' arose initially in connection with minors issued with cautions[6] but who remain classified as 'suspected offenders' on PULSE. AGS confirmed this is the same classification as minors charged and convicted who would also remain marked as 'suspected offenders'.

The Team requested clarification on the category 'suspected offender'. AGS clarified to the Team that when a 'Person' is recorded on PULSE in association with an incident, an appropriate 'role' will be selected from the available predefined list of Person Roles for an incident (e.g. "Suspected Offender" would be selected for the record of a person that AGS suspected of having committed the offence and where there was sufficient admissible evidence to warrant recording the incident as detected and having been committed by that person).

On the day of the inspection of Donnybrook garda station, AGS clarified to the Team that, in order for a charge sheet to be generated or a summons to be issued, an individual must be classified on PULSE as a 'suspected offender'. Otherwise AGS cannot progress to generate the charge sheet. AGS stressed during subsequent discussion on this classification that the role of 'suspected offender' being attributed to a 'Person' is crucial where an incident has been detected. The Team enquired why a person could not be classified with the role of 'suspect' when being charged and AGS responded that the key difference between whether a person is recorded as a

[5] AGS indicated that HQ Directive 11/2003 and extract from PULSE User Manual Procedures and Responsibilities Second Edition, 2001 provide additional detail on procedures for persons arrested and persons detained.

[6] AGS further clarified that where a minor has been dealt with by way of 'Caution' under the Juvenile Diversion Programme, the 'Suspected Offender's Detection Status' for that incident, will be recorded as 'JLO – Caution'. Where a minor is not offered a caution or rejects the offer of a caution and is charged and subsequently convicted, the 'Suspected Offender's Detection Status' for that incident, will be recorded as 'Completed'.

'Suspect' or a 'Suspected Offender' depends on whether the incident is marked as detected or not. The Team ascertained that if an incident is marked as 'detected' this means AGS consider there is sufficient admissible evidence to warrant recording the incident as 'detected' and having been committed by that person. AGS reiterated that charge(s) can only be pressed or a summons issued if the role of 'suspected offender' is assigned.

The ODPC raised the issue of the dual use of the categories "suspected offender" and "summons issued". AGS in response clarified that the status of a summons application on PULSE will indicate whether the summons was issued or not. For the purpose of generating a summons application the incident must be marked as detected and a person role of 'Suspected Offender' must be selected.

AGS stated that if the 'Suspected Offender' is subsequently not convicted of the criminal offence, the role of the person within that incident and the detection status of the incident may be changed to reflect that the individual is no longer a suspected offender in the case e.g. a court outcome where a person is acquitted. However, if AGS believed the person was still a suspected offender and the court case was not successful due to insufficient evidence the role of 'suspected offender' would remain on PULSE. AGS clarified that if a case is struck out in court, the individual concerned will still remain classified as a 'suspected offender'. The Team enquired as to what "detection status" would be entered where a case was struck out. AGS clarified that on completion of a court case the suspected offender's 'Detection Status' for that incident will be marked as 'Complete'. The court outcome linked to the suspected offender will reflect the result of the court case for that specific offence.

"Witness"
AGS Mullingar outlined to the Team that someone who is initially classified within PULSE as a 'suspect' but eventually cleared of any wrongdoing may have their record changed to "Witness". Equally, someone who is initially classified within PULSE as a 'suspected' offender but eventually cleared of any wrongdoing may have their record changed to "Witness." The Team viewed evidence of this policy in practice when examining the custody record of an individual who was arrested for drunk driving and assigned the role of 'suspected offender' because in this case the incident was detected by AGS as they stopped and breathalysed the driver. Subsequently in the station it transpired that the driver's sample was in fact under the legal limit. In this instance the driver's categorisation was changed to 'witness.'

During the inspection of Mullingar AGS it was indicated to the Team that if a person was arrested under section 12 of the Mental Health Act they would also be entered as a 'witness' on PULSE. A subsequent discussion in this regard took place between the Team and AGS Donnybrook. The categorisation of a person detained under the Mental Health Act as 'witness' on PULSE was noted by the Team but on the day of the Donnybrook inspection the Team noted an incident category- **'person** The Team referred to the PULSE Manual which depicted a number of scenarios associated with this category

"Person Misadventure"
Dead body - no offence disclosed
Defib
Industrial accident (fatal)
Industrial accident (non fatal)
Mental health act (detained under)
Missing person high risk (formerly category a)
Missing person medium risk (formerly category b)

Missing person low risk (formerly category c)
Missing person found (no longer an incident on pulse - historical incidents only)
Sudden death
Suicide
Suicide (attempt only)
Unidentified person (alive)
Unidentified person (deceased)

"Questioned in relation to"
As outlined previously, AGS also clarified that a person can have more than one role in an incident e.g. it is possible for a person to have a role of 'Questioned in relation to' and to have an additional role of 'Suspect Offender' added at a later stage as the incident / investigation progresses.

AGS Donnybrook also described a scenario where a vehicle is stopped and searched and drugs are found in the vehicle. The occupants of the vehicle might initially be marked on PULSE as 'suspected offender (s)' but if no drugs were found on their person(s) then this category would be changed on PULSE to 'searched'.

The Team queried whether the previous categorisation of Q.I.R.T.O would be visible in the **'History'** area of PULSE which captures and documents all text entered at each stage of the record and subsequent amendments/re-categorisations. AGS in response outlined that the 'History' functionality on a PULSE incident will record and save all information documented in the narrative field **only**. The 'History' functionality does **not** record any amendments to the person's role in the Person tab.

Another example of follow-up regarding classifications on PULSE was provided to the Team by AGS where a car originally believed to be stolen was actually borrowed by a family member. AGS outlined that a vehicle that has been reported as 'Stolen /Taken' will be recorded on PULSE with a role of 'Unauthorised Taking'. In the scenario described where it transpired that the vehicle had not in fact been taken, then the incident would remain on PULSE but would be updated to ensure the vehicle status of 'Unauthorised Taking' is removed and the record of the vehicle being stolen 'invalidated' to ensure the incident was not counted as a crime.

The Team subsequently examined the invalidation process in detail during its inspection of GISC[7] in Castlebar. The Team was informed that a GISC reviewer can 'invalidate' a record but only based on a member's instruction. GISC clarified that invalidated records remain on PULSE but are clearly marked as invalidated records and the reason is given as to why the record was invalidated. GISC also demonstrated to the Team how PULSE shows the entire history of narratives on PULSE including the narratives that are overwritten when a record is invalidated.

The Team examined an interesting example of a record which a member had requested be marked invalid in Dec 2012. This case concerned an allegation that electrical household goods had been removed from a house which had been repossessed by a bank. This was reported to AGS in 2009 by the bank. GISC outlined that it had subsequently transpired that the occupier of the house was entitled to remove the goods. GISC demonstrated how the member had not initially marked the individual accused as a 'suspect offender'. The Team noted only the name and address of the individual was in the narrative only. GISC/AGS cited this as an example of good practice given the sensitivity and volumes in recent times of such incidents and the likelihood that the individual may have done nothing illegal.

[7] Garda Information Services Centre

On the day of the inspection of Mullingar AGS the Team noted a section on PULSE entitled **'GPS Coordinates'** – and was informed the geographic coordinates are recorded based on the location of the incident and that they are used by the Analysis Unit in Crime Policy, AGS for the analysis of crime statistics and also by the Road Safety Authority. Later, during the course of the GISC inspection in Castlebar, GISC referred to the importance of GPS coordinates being entered when recording incidents on PULSE. GISC also referred to future plans within AGS to use GPS co-ordinates in a far more precise manner such as down to the level of individual properties.

It is recommended that AGS engage further with the ODPC on the use of GPS co-ordinates when plans for their deployment are at proposal stage.

"Attention & Complaints"

The Team, during the course of the Mullingar inspection, also queried the category **'Attention & Complaints'** on PULSE. AGS outlined that historically AGS had maintained a hardcopy 'Occurrences' book. In both instances, AGS maintained that the recording of anything that might prove useful under the category **'Attention & Complaints'** was often of significant assistance to them. AGS cited an example where a woman rang a garda station to say she heard three loud bangs but was not sure were they gunfire shots or not. AGS indicated this would be recorded along with the caller's name for future reference should any similar or connected incident come to the attention of AGS in this regard.

4.4 Intelligence on PULSE and Criminal Intelligence Officers

The Audit Team ascertained that PULSE is not just used to record crimes or offences. The PULSE system is used to record all 'incidents' that come to the attention of AGS including routine intelligence reports.

> An example of the role routine intelligence can play in assisting AGS was provided to the Audit Team when viewing a record on PULSE of a man who as a minor had been issued with two formal cautions. The man's record contained 54 pieces of intelligence - one recent entry being that at 6.10am one morning his car was stopped by AGS and a bolt cutter found in the back of the boot. This was not entered as an 'incident' onto PULSE because AGS determined that, he did not have any criminal intentions at that immediate point in time. However, the intelligence regarding the fact of a bolt cutter being present in his boot was relevant and was therefore entered onto PULSE.

In terms of intelligence-based entries onto PULSE, as opposed to incidents, AGS indicated that currently these types of reports are sent to criminal intelligence officers (CIOs) working within each garda district who review and proceed to approve their input if they are deemed to be intelligence reports appropriate to PULSE.

The Team met with the PULSE criminal intelligence officers for AGS Mullingar and Donnybrook who both outlined that it is the members of An Garda Síochána who create intelligence on PULSE and the CIOs who review this intelligence as opposed to the CIOs creating intelligence themselves.

The CIO in Donnybrook AGS explained to the Team that they do not review 'incidents' entered by members onto PULSE in terms of data quality etc reiterating that CIOs only review 'intelligence' entered on PULSE. In terms of the review role of C.I.Os, the CIO indicated she would review all intelligence created with a view to ensuring its quality and completeness before approving/removing it. The CIO outlined that the CIOs role is not to validate/invalidate intelligence but to work with members and interrogate the members more to make each piece of intelligence being created more valuable and precise. The CIO confirmed that she could also invalidate intelligence if deemed necessary.

The CIO in AGS Donnybrook confirmed to the Team that CIOs can create warnings, associations and register interests in persons, vehicles etc but the CIO in Donnybrook station stated that in practice she did not 'register interests' (see 4.4.2 below).

AGS clarified to the Team that intelligence records on PULSE are not subject to time limits. The CIO in Mullingar station clarified to the Team that she may have to review intelligence being created regarding a sexual offence but would not be able to view who the alleged offender was.

AGS clarified that 'Warnings' created on PULSE are subject to time limits.

The ODPC is aware that routine intelligence gathering is core to AGS in terms of performing its policing function. We do not challenge the role of AGS in observing and recording all incidents and sightings considered noteworthy onto PULSE. We acknowledge that the recording of all such observations may not necessarily involve the commission of crime or lead to its detection, but may be of use to AGS in building a case against the activities and movements of individuals over time. In terms of the review, retention and disposal of intelligence held on PULSE, the ODPC considers that AGS policy with regard to the retention of certain categories of intelligence should be examined by AGS in conjunction with the ODPC.

The ODPC understands that a framework has been developed in the UK and outlined in **'Guidance on the Management of Police Information'** produced by the National Policing Improvement Agency (2nd ed, 2010). The ODPC notes the reference within this guidance to the operation of 'clear periods' where a retention period for intelligence records is set at the end of which the relevant records are reviewed and either deleted or retained for a further period after which they will be once again subject to review.

4.4.1 Warnings

AGS outlined that a warning is used in PULSE to flag something e.g. a warrant out for someone's arrest or someone wanted for questioning, someone who is noted as being very aggressive, or there is a barring order on them entering a property such as the former family home.
The Team enquired as to whether AGS had issued any guidance in relation to warnings being entered on PULSE as to their appropriateness and AGS referred to **PULSE User Manual Procedures and Responsibilities Release 2 Edition**. AGS stated that these User Manual Procedures provide guidance for members creating warnings on PULSE.

AGS outlined to the Team that garda Members may create a warning on any item of interest linked to an intelligence record. This warning will only remain valid for a period of 120 hours (the duration of the warning has been recently increased from 4 to 5 days due to changes to the Garda Rosters). The Garda Member may request

the Criminal Intelligence Officer (CIO) to extend the duration of a warning. To have a warning extended the Garda member will make contact with his/her local CIO and discuss the matter and may have it extended for a period of up to one month. The District Officer can authorise the continuance of a warning for a period of three months.

AGS clarified that if a 'warning' is attached to a domestic violence order, the warning will remain on the system for as long as the order lasts.

In terms of warnings, the CIO in Mullingar AGS outlined that she would not generally create 'personal' warnings but would create warnings on vehicles. AGS clarified that a CIO may create a warning on any items of interest (vehicle, persons, objects, organisations) linked to an intelligence record for a period deemed necessary. In addition, there is a facility on the Garda Portal for CIO's to publish Criminal Intelligence Bulletins relative to their locality.

The Team viewed a number of warnings on the portal that were local to Mullingar.

4.4.2 "Registered Interests"

AGS outlined that the Registered Interest system is predominantly used by CIOs but is available to all members on application through their Superintendent and on approval by D/Chief Superintendent Security and Intelligence. The purpose of the "Registered Interests" system is to assist members in crime investigation and intelligence gathering. The system allows members to record their interest on PULSE in an 'Item of Interest' (IOI), i.e. person, vehicle, object, location, organisation and/or incident. Having registered an interest on a specific item, the member will be advised, by way of a screen message, of any update activity relating to an item in which he/she has registered an interest. The member can check the particular item to see the type of activity that has taken place. AGS stated that members are confined to a maximum of twelve registered interest at any one time.

AGS stated that generally all CIOs who are situated in Garda districts across the country would create and record registered interests in PULSE. AGS confirmed that all CIOs are permitted access to registered interests.

The CIO in Mullingar station demonstrated how she would 'register an interest' in certain pieces of intelligence for example on foot of a vehicle warning. This vehicle would subsequently be recorded in PULSE as a 'registered interest' and any updates regarding that vehicle would be made available to anyone who had registered an interest in it on PULSE.

AGS outlined that a flag will go up in PULSE if something regarding a registered interest is activated and all members who are recorded as having registered an interest in that item will be alerted.

For example, AGS demonstrated to the Team how they might register an interest in a prominent criminal figure and a flag would be activated in the system alerting all users who have registered an interest in this person.

4.4.3 Criminal Intelligence Bulletins

The Team viewed some Criminal Intelligence Bulletins on the Garda portal and the CIO demonstrated how she would create a bulletin based on a photograph of someone who had already been captured on PULSE. These Criminal Intelligence Bulletins were visible nationwide.

AGS stated to the Team that all Criminal Intelligence Bulletins and Caught on Camera CCTV footage must have a corresponding PULSE Incident. AGS clarified that CCTV footage of insufficient quality to identify suspects will not be published on the Garda Portal. Any footage that is not the subject of a National Intelligence Bulletin will be placed on the 'Caught on Camera' section where the identity of those suspected of commission of the crime under investigation are unknown.

In a case where the identity of an individual is being sought, intelligence can be circulated on the Garda Portal through; National Criminal Intelligence bulletins, Caught on Camera or Local Criminal Intelligence bulletins. Local bulletins are designed to attract immediate Garda District audience but are available to all portal users. AGS outlined that in general, the method of circulation depends on the purpose for which the information /image is being circulated (e.g. identification sought, whereabouts of individual sought, information in relation to particular individuals, safety advice or alert, etc), the seriousness of the offence, the quality of the image and the relevance to other Districts / Divisions.

4.5 Use of PULSE

AGS Mullingar outlined to the Team that in line with AGS policy the record of the incident itself which has led to the individual's arrest or detention should be created on PULSE by Garda Information Services Centre (GISC) in Castlebar[8]. AGS indicated that each member must ensure the incident is on PULSE within either the completion of the member's tour of duty, within twenty four hours or prior to commencement of proceedings (see table in section 4.3). AGS stated there was a HQ Directive in this regard - HQ 18/2007 GISC - and indicated that PULSE User Manual Procedures and Responsibilities Second Edition, 2001 also refers.

On the day of the GISC inspection, GISC estimated that of the 90% of members using GISC across the board, 33% of the incidents are now recorded when the members return to the station before completion of their tour of duty. GISC considered this was a significant reduction from the previous rate of members using GISC (before completion of their tour of duty) which was circa 70%. GISC concluded that this demonstrated the extent to which members had learned to engage with GISC as soon as possible after an incident occurred.

AGS indicated that a charge sheet cannot be prepared if an incident hasn't yet been entered onto PULSE and that it was the Garda member's responsibility to ensure an incident is entered onto PULSE (the member's Sergeant also has responsibilities in a supervisory capacity). Thus, if a prisoner is in custody and the relevant Sergeant wants to print the charge sheet, the PULSE entry must be created and reviewed by GISC as a matter of priority. GISC confirmed to the Team that it is the case that GISC reviewed all such incidents where charges were pending.

The Team requested statistics on the percentage of incidents created on PULSE by GISC on behalf of AGS Mullingar District and AGS Donnybrook over a three month period.

[8] GISC is the chief contact centre for operational members of An Garda Síochána. GISC was established to allow members of AGS to log all incident data over the phone with GISC instead of the members having to wait to return to their station to input or update data on PULSE. GISC was established on a pilot basis in September 2005 and rolled out nationally in October 2006 (see section 12 of this report).

GISC supplied the following statistics on the percentage of incident created by GISC for both Mullingar and Donnybrook for August, September and October 2012 as these were readily available within the timeframe required.

Donnybrook District		**Mullingar District**	
August	75.5%	August	95.3%
September	70.9%	September	91.9%
October	71.2%	October	94.7%
Average	72.5%	Average	94.0%

4.6 Adult Cautions on PULSE

AGS outlined that the Adult Cautioning Scheme is a scheme approved by the Director of Public Prosecutions which came into force on the 1st February, 2006. The Scheme only applies to offences committed on or after the commencement date of 1st February 2006, and to persons aged 18 years and upwards. It is an alternative to the prosecution of certain persons against whom there is evidence of the commission of a scheduled criminal offence, where the prosecution of such offence is not required in the public interest.

The list of offences which are eligible for the Adult Cautioning Scheme are as follows:

Criminal Justice (Public Order) Act 1994
Section 4: Intoxication (being drunk) in a public place
Section 5: Disorderly conduct in a public place
Section 6: Threatening, abusive or insulting behaviour in a public place
Section 8: Failure to comply with a direction (order) of a Garda
Section 9: Wilful obstruction (deliberate obstruction)
Section 11: Entering a building etc. with intent to commit an offence
Section 22: Surrender and seizure of alcohol.

Criminal Justice (Theft and Fraud Offences) Act 2001
Section 4: Theft - where the value of the property doesn't exceed €1000

Intoxicating Liquor Act 2003
Section 6: Offences by a drunken person

Section 8: Disorderly conduct

Non Fatal Offences Against The Persons Act 1997
Section 2: Assault - minor assaults (Assaults on members of the Gardaí are forwarded to the Director of Public Prosecutions for consideration)

Criminal Damage Act 1991
Section 2: Damaging property where the value of the property damaged is less than €1,000

Section 3: Threat to damage property.

AGS outlined to the Team that an adult caution is issued in person to an individual by a Superintendent with the agreement of the individual as an alternative to a prosecution. The individual is also informed that a record of this caution will be held on PULSE. The Team also noted that the document supplied by AGS **'Adult**

Caution – Decision to Prosecute' states that if a decision is taken to prosecute "the Garda must be in a position to inform the Court that adult caution was considered".

AGS indicated that an adult caution is often issued after an individual is released and the individual will be required to subsequently present at the Garda Station where the caution will be issued and signed.

The Team agreed to examine the procedures around the issuing of cautions as part of its inspection of a Garda station. During its inspection of Mullingar garda station, AGS provided the Team with a copy of the **Adult Caution Referral Form** which is completed by AGS and signed by individuals who are issued with an adult caution. The Team noted the individual must sign a statement which is worded

> "I understand that the details of an Adult Caution is recorded and may be made known to a court in the event of a conviction for another offence"

AGS referred to two HQ Directives - 6/2006 & 146/2009 - as providing guidance in relation to the Adult Caution Scheme. AGS also referred to the summary of the Adult Caution Scheme available on the Garda Website[9]. The Team was also provided with a copy of a document entitled 'Adult Caution Procedure'.

The Team noted the Adult Caution Referral Form stated that following the issuing of the caution, the original copy of the form is filed and retained at the District Office, with a second copy retained and filed by the recording station and a third copy furnished to the offender. In addition, the adult caution is recorded on PULSE, selected at the **'Detection Status'** drop down menu in the **'Person'** tab on the Incident screen on PULSE. AGS clarified that PULSE can be updated in this regard by the detecting member.

AGS stated to the Team that a second adult caution could not be issued to a person unless permission was given by the DPP. AGS confirmed that the record of an adult caution (first and second) would not be disclosed a part of a Garda vetting disclosure.

The Team noted that section E of the **Adult Caution Referral Form** requires the signature of the individual accepting or refusing to be considered for an Adult Caution on the understanding that they may be considered for an adult caution **prior** to submission to the Office of the Director of Public Prosecutions (DPP).

In this respect, the Team noted that section F of the **Adult Caution Referral Form** states

> I recommend that this referral form should be forwarded to the Director of Public Prosecutions for consideration (state reasons clearly)

The Team enquired under what circumstances would a form be forwarded to the DPP and AGS outlined that an Adult Caution referral form will be forwarded to the DPP under the following circumstances; A District Officer **may** seek directions from the DPP if s/he considers it to be an appropriate response to the commission of the offence or in the event that the victim is opposed to an Adult Caution. A District Officer **must** seek directions in the case of a subsequent offence being considered to be dealt with by way of the adult caution scheme and in the case of an assault on a member of An Garda Síochána.

---

9 http://www.garda.ie/Documents/User/Adult%20Cautioning%20final%20for%20publication.pdf

In terms of vetting and the issue of spent convictions, the Team wished to establish the basis behind the policy of the indefinite retention of records pertaining to cautions. AGS clarified that a caution would not be held against a person or disclosed in a vetting disclosure but considered it necessary to hold a record of the caution for the reason stated on the Adult caution Referral Form which the data subject signs

> "I understand that the details of an Adult Caution is recorded and may be made known to a court in the event of a conviction for another offence".

The issue of the retention of cautions and the disclosure of old and minor convictions is addressed in further detail in section 12 below in the context of the current situation and possible changes to the regime with new legislation due to be introduced with regard to spent convictions and the proposed disclosure of 'soft information' such as a caution in certain circumstances. The ODPC accepts that currently AGS has no legislation providing for the length of time a caution remains valid. The ODPC welcomes the fact that this matter is currently under consideration as part of the provisions contained in the Criminal Justice (Spent Convictions) Bill 2012.

4. 7 Minors on PULSE

The Team noted that on 16 October 2006, under the Children Act 2001, the age of criminal responsibility was effectively raised from 7 to 12 years. Under the new provisions, no child under the age of 12 years can be charged with an offence. An exception is made for 10 and 11 year-olds charged with very serious offences, such as unlawful killing, a rape offence or aggravated sexual assault. In addition, the Director of Public Prosecutions must give consent for any child under the age of 14 years to be charged.

The Team enquired in what instances are the details of children recorded onto PULSE and AGS responded as follows:

"A child of any age can be entered on PULSE (E.g. an injured party). PULSE Incident validation was updated in accordance with the Children Act, 2001 (as amended by the Criminal Justice Act 2006). PULSE Incident validation prevents a charge from being created for a child under 12 years of age except in the case where a child aged 10 or 11 years had committed an offence of Murder, Manslaughter, Rape, Rape Under Section 4 of the Criminal Law (Rape)(Amendment) Act 1990 or Aggravated Sexual Assault. (Sec 52 Children Act, 2001 as substituted by Sec 129 of the Criminal Justice Act 2006 -Restriction on Criminal proceedings against children."

Cautions issued to Minors

AGS stated that in the case of a minor (a person under 18 years of age) being issued with a caution this process would be overseen and issued by a Juvenile Liaison Officer (JLO) - a divisional based role which could cover a number of districts. Alternatively an Inspector could also issue a caution to a minor.

AGS stated that there are two different forms used to caution minors. The first form allows the minor to accept an 'Informal Caution' under the Diversion Programme for the alleged offence; the second form allows the minor to accept a 'Formal Caution' under the Diversion Programme. Both forms are signed in the presence of Parent/Guardian. There is a section on both these forms for the minor to formally decline to be accepted as part of the Diversion Programme.

Subsequent to the inspection, AGS provided supplementary information on the work of JLOs and the operation of its **'Diversion Programme'** - a statutory option

provided for under the Children Act 2001 to address the offending behaviour of children between the age of 10 years and 18 years.

AGS clarified to the Team that when issued with an Informal Caution a minor will sign an 'Acceptance / Non Acceptance of Inclusion into the Diversion Programme' Form stating that they accept an Informal Caution under the Diversion Programme for the alleged offence.

AGS also provided a copy of the 2011 report of the Monitoring Committee of the Diversion Programme and the Team noted the total number of incidents referred to the Diversion Programme during 2011 was 27,384, with 12,809 individual children referred to the Programme. In terms of the breakdown of informal and formal cautions for 2011, based on the total number of referrals 54% of children had their cases dealt with by way of an informal caution and 22% of children had their cases dealt with by way of a formal caution. AGS clarified that the remaining children referred are processed outside of the Juvenile Diversion Programme.

AGS clarified that if a minor is issued with an Informal Caution this will be recorded on PULSE as 'Informal Caution' under the 'Caution' tab linked to the relevant incident and Youth referral.

As an example, AGS also provided the Team with a screenshot from PULSE of a national youth referral form which displayed details recorded regarding an offence categorised as 'Trespass' where juveniles were found in the bedroom of the 3rd floor of a house that was recently abandoned.

In terms of vetting and the issue of spent convictions, the Team wished to establish the basis behind the policy of the indefinite retention of records pertaining to cautions issued to minors. AGS clarified that a caution issued to a minor would not be held against a person or disclosed in a vetting disclosure but considered it necessary to hold a record of the caution for the reason stated on the Youth Referral Form which the data subject signs

> "I realise that if I commit any offence in the future that I may be prosecuted for such offence and the details of my inclusion into the Diversion Programme in relation to this case may be given in Court at the time of the sentencing (Section 126(2) of the Criminal Justice Act 2006 refers)".

Subsequent to the inspection, the Team also came across a document on AGS website entitled **'Recording Procedures and guidelines relating to children in the care of An Garda Síochána'** which refers to '**An Garda Síochána Child Care Form'** which must be completed for every child that comes into Garda care (who is not arrested/detained). AGS clarified that the 'An Garda Síochána Child Care Form' refers to a manual record that is stored manually on and is not recorded/replicated on PULSE.)

Convictions of Minors

In relation to conviction information for minors, AGS referred to section 258 of the Children's Act 2001 and the fact that all previous convictions of minors cannot be viewed on PULSE in general. AGS also confirmed that PULSE has the necessary functionality in place to adhere to the non-disclosure of criminal convictions of minor offenders provided for in section 258 of the Children's Act 2001 once specific conditions outlined in the provision have been met. During the course of the audit the Team was satisfied that this functionality was in operation.

The ODPC also noted a briefing report on section 258 of the Children's Act 2001 produced by the Irish Penal Reform Trust[10] which stated

> "Section 258 of the Children Act 2001 provides that offences committed by those under eighteen years of age can be expunged from the record once certain conditions are met. Essentially, where a person has been found guilty of an offence and (i) the offence was committed before they reached the age of eighteen years, (ii) the offence is not one required to be tried by the Central Criminal Court (such as murder or rape), (iii) three years have elapsed since the finding of guilt and (iv) the person has not been dealt with for an offence in that three-year period, then that person will be treated as a person who has not committed or been charged with or prosecuted for or found guilty of or dealt with for that offence. Section 258 is fully retrospective so it applies whether the offence occurred before or after the coming into force of the 2001 Act.
>
> Individuals who come within the terms of section 258 are "treated for all purposes in law as a person who has not committed or been charged with or prosecuted for or found guilty of or dealt with" for the offence(s) in question[11]. As people meeting these conditions are no longer regarded under Irish Law as having committed an offence they essentially have a clean record and therefore, in the context of seeking employment or applying for an educational course or insurance, can truthfully claim to have a clean record[12].

Children at Risk

During the course of the AGS Mullingar station inspection, the Team encountered copies of the notifications received by AGS Mullingar from the HSE in relation to children and also the notifications AGS issues to the HSE regarding children they encounter offending - for example possession of drugs, public disorder. AGS confirmed to the Team that every HSE referral it receives is entered onto PULSE and any alleged sex offences or suspicion of child abuse or neglect will be followed up by AGS.

AGS stated in the first instance that the exchange of information between the HSE and An Garda Síochána is done solely for the welfare and protection of the child.

The Team also noted the requirement to notify the HSE in a policy document located on the AGS website entitled **'An Garda Síochána Policy on the Investigation of sexual crimes against Children and Child Welfare, 2010'**

> **29.5.** Where a child has been involved in the commission of a criminal offence, particularly where a child has been arrested, members should always consider notifying the HSE in accordance with the Children First guidelines.

Equally, the Team noted the policy states

> **31.5.1.** Where the HSE suspects that a child has been or is being physically or sexually abused or wilfully neglected, the HSE have a responsibility to notify An Garda Síochána

---

[10] www.iprt.ie/.../IPRT_Briefing_on_Criminal_Records_under_18_040112.docx

[11] See section 258(4)(c) of the Children Act 2001. See also Law Reform Commission, Report on Spent Convictions (Dublin: LRC 84-2007, July 2007) p. 53.

[12] See section 258(4)(c) of the Children Act 2001.

The ODPC noted a report produced in 2010 by the Garda Inspectorate entitled **Responding to Child Sexual Abuse** showed that in the years 2007 to 2009 inclusive, there were 16,073 child protection notifications issued between the Garda Síochána and the HSE, with the majority of them 11,472 (71%) being issued from the Garda Síochána to the HSE[13].

In terms of the mandatory recording of child sexual crimes the Team examined **'An Garda Síochána Policy on the Investigation of sexual crimes against Children and Child Welfare, 2010'** and noted the following:

> **5. Reporting & Recording**
>
> **5.1.** All reports of sexual crime must be recorded as outlined in Code Chapter 33[14].
>
> **5.2.** Recording Sexual Crime on PULSE
>
> **5.2.1.** On receipt of a complaint the member receiving same will immediately create the appropriate entry on the PULSE system, clearly identifying the reported offence.
>
> **5.2.2.** If at a later stage evidence becomes available indicating that the originally reported offence did not in fact occur, then the matter can be re-categorised or invalidated accordingly. It is imperative that offences are recorded accurately on PULSE.
>
> **5.2.3.** Divisionally appointed Inspectors will have responsibility for ensuring that all sexual crime incidents are properly recorded and reviewed on PULSE. S/he will review each report on a regular basis and notify the District Officer of matters requiring his attention.

In terms of the investigation of children where there was no suspicion that a sexual crime was involved but a suspicion of suspected abuse or neglect GISC referred to the section of the PULSE Manual dealing with the recoding of such notifications – '**Formal Notification to the HSE'** and '**Informal Consultation from the H.S.E.'**. The Team examined these excerpts and noted that for the **'Informal Consultation from the H.S.E.**' the PULSE manual stated

> "This incident type is used to record that an informal consultation has taken place between the H.S.E. and the Gardaí in relation to a case of suspected abuse or neglect. "

The Team also noted

> "A separate incident is required for each child if more than one child is involved".

and

> "The child should be recorded with a Role of 'H.S.E. Notification Concerning"

With regard to the **'Formal Notification to the HSE'** section of the PULSE manual the Team noted

[13] http://www.gsinsp.ie/index.php?option=com_docman&Itemid=39
[14] Garda Code of Practice

> "This incident type is used to record that the Gardaí have formally notified the H.S.E. that they suspect some form of abuse or neglect is taking place with regard to a child under 18 years of age and need to have it investigated or substantiated. A crime may or may not be established.
>
> If the Gardaí believe that a crime occurred, then a crime incident should also be created." (p 93)

The Team noted that if a crime occurred this is notified to the HSE

> "If a crime is established, create crime incident, create case and add all incidents to case. Record PID of crime incident in Narrative of Formal Notification to the H.S.E. incident" (p.93)

AGS clarified to the Team that PULSE provides functionality to restrict access to the following HSE incident types; Formal Notification to the H.S.E., Informal Consultation with the H.S.E., Formal Notification from the H.S.E. & Informal Consultation from the H.S.E. This access is restricted to the Investigating Garda, members not below the rank of Inspector and certain other members who have been granted permission based on an application (ITSU2) approved by their local District Officer.

The ODPC indicated it remained unsure as to the rationale for AGS to inform the HSE if a 10 year old (below the criminal age of responsibility) had been found shoplifting. AGS in response stated that "it is the responsibility of the responding Garda to make the decision as to whether the child's welfare or protection is at risk. The *Children First* guidelines state that the HSE Children and Family Services should always be informed when a person has reasonable grounds for concern that a child may have been, is being or is at risk of being abused or neglected. In the case outlined where a ten year old child has been found shoplifting it may be necessary to inform the HSE where the specific circumstances of the incident raise reasonable grounds for concerns relating to the child's welfare".

4.8 Access to PULSE

A key focus of the audit was to address a concern on the part of the ODPC, arising from complaints received to the Office, that there was insufficient oversight of those approved to access PULSE. The need to identify inappropriate access and therefore effectively discourage such access was outlined in the letter of intention to audit issued to AGS

> "Unfortunately, it seems to be the case at the present that the Gardaí are not in a position to identify, on a pro-active basis, inappropriate access to personal data held by it. Even in cases where complaints are received by this Office of inappropriate access by members of the force to PULSE, the investigations conducted by the Gardaí have taken an unacceptably long time to conduct and have rarely led to conclusions of inappropriate access by individual members.
>
> I have a statutory duty to ensure that personal data in the holding of all organisations, big and small, is handled in line with the requirements of the Data Protection Acts. At present, I am not in a position to fully assure the public that their personal data held by the Gardaí is handled in line with the requirements of the Acts."

The Team was informed that each time a member of AGS logs into PULSE a data protection notice appears to which each member must click 'ok' in order to proceed.

Standard Notification

> "This system is to be used for authorised policing purposes only. Unauthorised access or activity is a violation of An Garda Síochána policy and may be a violation of the law. All activity on this system is subject to monitoring in case of possible security violations."

A second notice then appears and the Team observed that if this notice wasn't acknowledged the system would time out and fail to grant access.

Data Protection is the safeguarding of the rights of all individuals to privacy and integrity in relation to the processing of their personal data.

DATA PROTECTION RULES ALL STAFF OF AN GARDA SÍOCHÁNA MUST ADHERE TO:

1. Obtain and process information fairly
2. Keep it only for one or more specified, explicit and lawful purposes
3. Use and disclose it only in ways compatible with these purposes
4. Keep it safe and secure
5. Keep it accurate, complete and up-to-date
6. Ensure that it is adequate, relevant and not excessive
7. Retain it for no longer than is necessary for the purpose or purposes
8. Give a copy of his/her personal data to the relevant individual, on request. Requests for personal data are managed by Superintendent, Data Protection Processing Unit, Garda Central Vetting Unit, Racecourse Road, Thurles, Co. Tipperary

Accessing or ***Disclosing*** personal data for any purpose other than that for which it was obtained is strictly prohibited. It is inappropriate to release data in the possession of An Garda Síochána to outside agencies or individuals, and such actions will subject members to full investigation in accordance with the Garda Síochána (Discipline) Regulations 2007.

While these standard notifications are helpful reminders to members of the AGS, the Team observed that they were of limited use if not accompanied by effective oversight and enforcement measures.

Audit Tool for PULSE

A key initial focus of the audit as outlined at the beginning of this report was to establish progress made in relation to discouraging inappropriate access to PULSE. At the commencement of the audit, AGS informed the Team that the proposed

system of audit and review of user access which was discussed extensively during its development was in place and was awaiting implementation. AGS stated that a pilot of the new system had been carried out in the Western Region. The Team was also supplied with a copy of the notification by email from AGS Professional Standards informing AGS internally of the initial pilot. The results of this were reviewed by the audit team during the course of the audit.

AGS acknowledged that previous audit plans were initially based on 'exceptional activity reports' as outlined in August 2011 at a meeting between AGS and ODPC when the first version of such a tool had been developed. Upon review and following the advice of this Office, the AGS informed the Team that it had decided that high volumes of usage were not necessarily the key indicator on which to base further scrutiny on a PULSE user or set of users. AGS made the point that a particular incident in an area may lead to legitimate spikes in activity and so the use of such an indicator might be misleading. AGS stated that as well as leading to an inefficient use of the audit tool itself, it did not wish to discourage productivity in terms of intelligence-based activities utilising PULSE.

AGS confirmed to the Team that the revised audit tool would allow a reviewer to check on all previous activity of a user if it was deemed necessary to query this. The review system places a responsibility on District Superintendents to require members to account for the business reason for a specified percentage of accesses to the system per month. These accesses are chosen at random by the review system and provided to the Superintendent in each case. AGS confirmed that the conduct of the review will be a performance requirement of each Superintendent with failure to do so leading to action.

Additionally, as part of the new audit structure of Garda access to PULSE, AGS stated that it intended that six districts out of a total of 105 districts would be audited per month by the Professional Standards Unit in AGS on a rolling basis. AGS referred the Team to HQ Directive 95/2012 'Data Protection in An Garda Síochána' stating that it outlines the process that will be followed in auditing Data Protection issues in An Garda Síochána. The ODPC welcomes the new audit structure put in place by AGS in this regard.

Search Functionality

The Team clarified with AGS that there was no functionality to hide a member of AGS on PULSE – serving, suspended or retired. In other words, if a member of An Garda Síochána had for example received an adult caution as a result of an incident or been the victim of a violent crime, this would be visible in PULSE. AGS confirmed that there was also no distinction made with regard to well known figures or high-profile celebrities. The Team referred to its audit of the Revenue Commissioners where provision was made to restrict the records of high profile individuals from general access. AGS acknowledged this as a potentially valid option but considered that the current settings on PULSE represented the democratic nature of the system in that nothing or no-one could be hidden on it (with the exception of some sex offender related data).

PULSE also contains a feature which requires persons looking up a person, vehicle or location to enter the reason for their enquiry. In 95% of the cases examined by the Team in November 2012 only the letter e (for enquiry) was entered. The policing reason for the introduction of this requirement was intelligence driven but its correct use would also serve the data protection requirement that persons with access to PULSE would need to enter the reason why they were accessing particular

information and thereby discourage inappropriate use. It was clear to the Audit Team therefore that the function was not serving its intended purpose.

AGS clarified that there is no feature (inquiry field) for a member of An Garda Síochána to enter a reason for their inquiry when looking up any PULSE 'Incident'. The feature (inquiry field) only applies to Person, Vehicle and Location searches.

AGS also stated that in some cases a member may not be able to look at a particular incident on PULSE such as previously outlined on page 20 where PULSE provides functionality to restrict access to certain HSE incident types; Formal Notification to the H.S.E., Informal Consultation with the H.S.E., Formal Notification from the H.S.E. & Informal Consultation from the H.S.E.

AGS clarified to the Team that the 'Previous Inquiries' functionality on PULSE does not show details of members accessing these restricted areas but indicated that the IT Section at Garda Headquarters could search and view information in this regard.

'Previous Enquiries'

During the course of the demonstration of PULSE, AGS demonstrated a search facility **'Previous Enquiries'** which allowed authorised users to enter the number of the member of AGS being queried and to view all the enquiries they made on the system. The ODPC considers this to be a very useful feature to have built-in to the system.

A key feature of PULSE is this transparency in terms of individual member access to incident details. Most modern IT systems today contain extensive logging mechanisms that allow for individual access to be interrogated following access. PULSE has this functionality but additionally there is a facility at the user front-end of the system which clearly outlines all accesses made by all members in relation to a record on PULSE and the reason entered by them for such accesses. AGS confirmed to the Team that the 'Item Previous Inquiry list' can be viewed by all members.

This facility actually provides a real-time basis for dealing with inappropriate access as it is the lead officer on a particular investigation who is best placed to raise a concern if they note access to an incident by persons who they consider may not otherwise have a business interest. Investigation Teams should be encouraged to monitor and raise any such accesses through the appropriate channels taking account of the fact that the confidentiality of such information is crucial from the perspective of an investigation as well as from a data protection perspective.

Sample Review

Assisted by AGS, the Team proceeded to conduct an extensive sample review of logs on PULSE in relation to access to the records of well known public figures and celebrities. Specific complaints received by members of the public were also examined. The Team identified what appeared to be inappropriate access on a surprising scale in relation to the public figures selected as outlined below:

Two high-profile persons whose details were recorded on PULSE in relation to minor offences or incidents where they were victims or witnesses had their records accessed over 80 and 50 times respectively by members of AGS. A review of these accesses by the Team led to the identification of the same Gardaí in several instances as having accessed both records. The Team also checked the PULSE records of three high profile media personalities and also a well known inter-county GAA player. The number of Pulse accesses returned appeared to bear no relation to the valid entries relating to these individuals in connection with official police business and again, there was commonality in the members who had looked up these individuals. Effectively, all the six i.e. 100% of the "high profile" personalities whose Pulse records were reviewed in detail by the Team apparently had their records inappropriately accessed by AGS members.

The ODPC considers these findings to be particularly disturbing given almost all the individuals selected had no known major dealings with AGS. The ODPC was able to verify this by checking the PULSE records of the individuals involved and while they may have reported a crime, e.g. in one instance an individual had reported stolen property, at no stage had any of the individuals concerned been categorised as an offender or suspect offender by AGS. As outlined previously in this report (see p.11) there are a range of other roles which may be assigned to a person such as 'injured party', 'witness', 'reported by' etc.

The ODPC fully recognises that the nature of policing work effectively requires members of AGS to check personal information on a regular basis. Notwithstanding this, it is imperative that inappropriate access be identified and dealt with so as to ensure that persons with access to PULSE respect the obligation that comes with that access.

In partial response to the above, (in any case it was already in train) and was referred to by AGS in advance of the audit, the Commissioner of An Garda Síochána issued HQ Directive 95/2012 'Data Protection in An Garda Síochána' to all members of the Force on 06 December 2012 which inter alia states "it is essential when enquiries are carried out on Items of Interest i.e. Persons Vehicles Locations, full information should be included in the "reason" for enquiry field in accordance with instructions at Code 32.15(3) and HQ Directive 14/2001. There will be no exceptions to this."

The ODPC welcomes this necessary development. This Office however expects An Garda Síochána to now actively enforce the terms of HQ Directive 95/2012 and take strong and appropriate disciplinary action against any persons abusing their access to PULSE and prosecutions against any person found to be using such access for gain.

4.9 Data Entry on PULSE: Garda Information Services Centre (GISC)

Most raw data entry on PULSE is done by GISC based on reports received from individual Garda members. In view of its key role in relation to the accuracy of data entered in PULSE it was the subject of a special inspection at its headquarters in Castlebar.

GISC was established to allow members of AGS to log all incident data over the phone with GISC instead of the members having to wait to return to their station to input or update data on PULSE. GISC was established on a pilot basis in September 2005 and rolled out nationally in October 2006.

The objectives of GISC as stated on the AGS website are to:

- Increase Garda visibility
- Reduce Garda administrative workload
- Improve the data quality on PULSE

GISC outlined to the Team that it currently has 190 staff (all civilian) including a Principal Officer who reports to the Assistant Commissioner in AGS who heads up the Organisation Development and Strategic Planning branch within AGS.

GISC stated to the Team that it handles 14-15,000 calls a week on average and that overall 90% of all data entered onto PULSE regarding incidents is completed by GISC. It confirmed that the user rate of Garda stations availing of GISC varies from 75-100% depending on the Garda district. The Team enquired as to statistics regarding usage of GISC for data entry on PULSE across the country and AGS provided the ODPC with a league table showing the percentage of incidents created by GISC for each District from January to October 2012.

GISC also operates two other minor services on behalf of AGS – '**Traffic Watch'** which GISC described as a facility for members of the public to report driving hazards or incidents of dangerous driving via a low-call telephone number. GISC stated that this hotline generates an average of 80 calls per week. GISC informed the Team that it also oversees an on-line reporting of theft facility - **Online Declaration'**[15] where the theft of property to the value of less than 500 euro can be reported online. GISC stated that this facility has only generated 200 emails in total since it was established in 2010.

In terms of the operation of their main function for serving AGS members, as soon as possible after an incident occurs, members are expected to contact GISC on their Tetra phones (which also function as Garda radios) over the Tetra communications network and give the incident details to trained civilian call-takers in GISC who enter the details onto the PULSE system. GISC confirmed to the Team that the GISC freephone number is no longer in use (thus members would not use their own mobile phones to call in incidents).

The Team outlined to GISC that on its previous inspections of Mullingar and Donnybrook stations, the Team had been assured that it was AGS official policy that all records of incidents leading to an individual's arrest or detention should be created on PULSE by GISC in Castlebar.

GISC stated that it operates on a 24/7 basis with three different split shifts in operation. GISC stated that the average time to capture incident data is approx 6 minutes. Typically GISC outlined there would be approximately 25 staff rostered per shift. Across the shifts there is a pool of 27 reviewers who cover the different shifts and review every entry created across the shift and to provide ongoing assistance to the Team during the shift. GISC described the reviewer's role as ensuring consistency in how incidents are categorised and enhance the accuracy of all data entered onto PULSE.

[15] http://www.Garda.ie/Controller.aspx?Page=4002&Lang=1

As well as GISC call operatives, reviewers and duty managers assigned to each shift, GISC also referred to its Systems and HR section. In terms of its Systems Section, GISC outlined that this section provided technical support liaising with Garda IT on a daily basis and it would conduct forecasting in terms of planning staff rotas and staff levels taking into account leave patterns etc in terms of peak policing times or key events. GISC also indicated it would liaise with AGS Crime Policy regarding classification issues on PULSE such as the distinction between an attempted burglary and a criminal damage incident.

Sexual Assaults/Sex Offences

GISC informed the Team that since October 2011, GISC staff had begun recording incidents of sexual assaults onto PULSE. GISC outlined that all staff in GISC had received specific training for this and that the entry created on PULSE in this regard goes to the reviewer in the normal way. GISC clarified to the Team that all GISC staff working as call operatives have access to these incidents as a member may ring back to update the record and staff would need access on this basis. GISC also stated that all staff working as call operatives had access to this data due to the call distribution system in place which distributed calls based on a queue system and this could not be overridden.

The Team asked AGS to provide more details as to the background governing the decision to provide access to this restricted area of PULSE to civilian staff in GISC given that access to this area is restricted in terms of access by rank and file members of AGS. GISC outlined that originally GISC was charged with recording all incidents but that due to the sensitive nature of Sexual Abuse Incidents, their data capture was placed outside of the remit of GISC. GISC stated that increasingly it became apparent that, when capturing data centrally through GISC agents in consultation with frontline Gardaí, the speed of capture allowed trained Garda staff to move from certain administrative functions to frontline policing. In 2010, certain legacy data was identified by the Garda Inspectorate and GISC were requested to ensure this data was accurately recorded on PULSE. Subsequently, after delivering to an acceptable standard, the Garda Inspectorate, in their Report on Responding to Child Sexual Abuse (2010) recommended that;

> "in the interest of Quality Assurance, the services of the Garda Information Service Centre (GISC) at Castlebar be used to enter records of sexual offences on PULSE." (Recommendation 27)

In October 2011, after GISC staff had received training on Sexual Incident data capture and review, Garda Management implemented this recommendation. GISC clarified that its role is specifically in relation to data capture and the quality assurance of that data against the Crime Counting Rules as distinct from the investigation of the incidents captured. GISC also stated that GISC staff are all civil servants working within AGS, who are bound by the Official Secrets Act and have been subject to full garda vetting and security clearance.

The Team asked AGS to outline exactly how sexual offences data is restricted within PULSE for members of AGS. AGS responded outlining that the incident narrative, incident scene and associated Garda members (e.g. investigating member's name and station) of incidents of a sexual nature are visible to all users that can view the details of a PULSE incident. Details of Person records and any other item that is linked to that incident are only visible to the investigating Garda member, members

not below the rank of Inspector, certain other members who have been granted permission based on an application (ITSU2) approved by their local District Officer and staff at GISC who create, update and review the incidents.

The Team enquired as to what safeguards AGS put in place entering into this new arrangement with GISC and AGS responded stating that GISC is part of AGS, its staff report to the Garda Commissioner and the standards that apply to the organisation as a whole apply to GISC. AGS reiterated to the ODPC that senior management in AGS initially kept Sexual Abuse Incidents outside the scope of GISC until it was satisfied that this Unit in the Organisation could meet the targets set down on establishment and then awaited the assessment and recommendation of an independent body before extending GISC's scope by sanctioning the capture of Sexual Abuse Incident data. The Garda Inspectorate, following a rigorous examination of the best use of resources to respond to Child Sexual Abuse issues, concluded that GISC were best placed to oversee the data capture in regard to such incidents.

AGS outlined that the same safeguards apply to Sexual Offences as to all other incidents. The sole objective of GISC is to ensure all data is efficiently captured in line with the highest standards of accuracy. Specifically on Incident Creation, GISC is committed to answering 80% of calls within 20 seconds, handling calls in 6 minutes, on average, and quality assuring all data captured. AGS cited the Official Secrets Act as being a key safeguard to ensuring appropriate use of the data. AGS stated that reminders on confidentiality are issued by GISC management to all GISC staff on an ongoing basis.

In terms of review procedures, AGS stated that as a data product, all incidents captured by GISC are reviewed in house. Furthermore, all incidents under investigation are reviewed from a policing perspective at District Officer level and they are subject to scrutiny at Divisional, Regional and National level. The Internal Audit Unit within AGS has visited GISC on a number of occasions in the context of following up on issues arising in its various audits of other parts of AGS. GISC has also been visited by Assistant Commissioners and by the former Chief Administrative Officer.

The Team was also informed that the Garda Inspectorate has visited GISC on three occasions. Most recently, in February 2013, in the context of its examination of crime management and detection within AGS, the Inspectorate examined GISC's call handling, incident creation and review, Data Quality, CJIPP and Systems. It requested various reports on information held on PULSE. These were then supplied via the Assistant Commissioner, Organisation Development & Strategic Planning. The ODPC understands that the Garda Inspectorate will issue a report in due course.

GISC estimated to the Team that it received an average of 67 calls per week reporting, enquiring and updating incidents concerning sexual offences. GISC provided the Team with a copy of **'Sexual Offences – Recording Guidelines – 19th Oct 2011'**.

Upon review of the **Sexual Offences-Recording Guidelines** the Team noted that it is not AGS policy to record names, addresses or locations of persons involved in narratives. AGS referred to the **Garda Policy on Investigation of Sexual Crime, Crimes against Children and Child Welfare 2nd Edition, 2013**. Specifically, Chapter 5 of the policy in relation to the recording of Sexual Crime on PULSE states:

5.2.5. It is essential that all details are recorded in the PULSE incident concerned, including the PULSE ID of the complainant and the suspect. Such details are available on PULSE only to the investigating member for the incident concerned, members not below the rank of Inspector and certain other members who have been granted permission based on an application (ITSU2) approved by their local District Officer.

5.2.6. However, members should not put any information in the narrative, which could lead to the identification of the injured party. This includes name, address, or relationship to the culprit, if the culprit is named. The narrative of all incidents is available to operational members. This allows members to be aware of the general details regarding crime in their area.

5.2.7. When sexual offences are undetected, maximum offender details in the narrative are required. This is to assist operational members in identifying the culprit without disclosing the identity of the injured party. In all cases the investigating member and his or her station details will be available to the user who can seek additional details if required for operational reasons.

The Team recalled that during the Mullingar inspection, the Criminal Intelligence Officer (CIO) stated to the Team that she may have to review intelligence being created regarding a sexual offence (see section 4.4). Also, as outlined in section 5.1 the Team was told AGS rank and file would be able to see if someone who was arrested was on the sex offenders' register but wouldn't be able to actually search the sex offenders register. AGS reiterated that there is restricted access to incidents of a sexual nature on PULSE, however there would be no restrictions in relation to the information displayed in an intelligence record. The CIO would be able to see all the details in an intelligence record but may not necessarily have access to view the person details recorded in a PULSE incident of a sexual nature. The ODPC indicated to AGS it considered this to be good practice from a data protection perspective.

GISC Caller Operatives

The Team sat down with three different GISC staff members rostered that morning to take calls from members and create incidents on PULSE. The Team received a comprehensive demonstration of the level of additional data and clarification sought by the GISC caller operatives by listening to the calls taken and observing how the GISC caller operatives pushed the members at every point for more specific information. For example, the theft of a wallet or purse from a coat would be recorded as a 'Theft from Person' incident if the person was wearing the coat, while it would be recorded as a 'Theft Other' incident if the coat was left unattended hanging on a chair. The scenario where a person enters a shop, takes an item from the shelf and leaves the shop without paying for the item would be recorded as a Theft From Shop incident however, if the person took the same item from a shelf in the storage room of that shop, that the public did not have access to, the incident would be recorded as a Burglary incident.

Caller Verification

GISC outlined to the Team that each Garda has a Pulse PIN no, which they input prior to their call being dealt with. The call handler can see on their hand set whether the PIN has been verified but GISC clarified that the PIN itself is masked. If the incorrect PIN is entered a PIN 'Inaccurate Message' appears on the handset. At this stage the call handler checks the callers ID by checking some combination of the

following information which is available on the PULSE System: Full name, Reg No, Station, Unit and Shoulder No. GISC informed the Team that each GISC staff member also has a personal PULSE ID.

Duplicate Records

GISC outlined to the Team the importance of all incidents phoned in by members being matched up to any record relating to an individual which may be on PULSE already. Duplicate records may exist on a person within PULSE due for example to an error in the spelling of a name or a digit error in a DOB. The Team commented that it had observed many duplicate records during the course of several demonstrations and search exercises conducted on PULSE during the course of the audit.

In response, AGS stated that there have been a number of initiatives to deal with the issue of replicate records on PULSE. The PULSE Merge functionality was deployed in 2003 to deal with the issue of replicate Person and Location records. Divisional Merge Teams were set up as part of the process to identify, evaluate and create the merge requests for these replicate records. In 2004 technical issues impacted the merge process.

Revised 'Replicate Person Reports', designed to assist individuals at a local level identify potential replicate Person records on PULSE, were issued in 2007. These Person records are identified as potential replicate records based on the person's name, date of birth, address and local station and these reports are disseminated to the relevant District. These revised reports have been issued to the organisation on four occasions.

AGS clarified that overall responsibility for the PULSE Merge Process lies with the National Criminal Intelligence Officers in AGS HQ but that at a more local level the CIO or Sergeant may have a role to play in these tasks. AGS outlined that the key requirement was that there would be human intervention involved to ensure the merge was correct. AGS clarified that fingerprints are not built into this merge process but if a search of AFIS[16] is conducted and fingerprints have been submitted previously, AFIS will show a match and this knowledge could assist the member in determining whether a merge was the correct course of action.

Review Procedures

GISC demonstrated to the Team how every entry on PULSE must be checked by a "reviewer", including those input by GISC call-takers as well as any members of AGS who created the incident record themselves. GISC estimated that in the region of 13% of records created by members are sent back for clarification, with the main issue usually being that GPS coordinates weren't entered. GISC clarified that GPS co-ordinates are important in order for the AGS Crime Analysis unit to analyse and identify crime hot spots. GISC also referred to future plans within AGS to use GPS co-ordinates in a far more precise manner such as down to the level of individual properties.

Call Recordings

GISC informed that Team that all calls to GISC are recorded since Jan 2007 and are stored on the local site server. GISC confirmed that this data has been retained indefinitely up until now but GISC itself had recently decided they will have to review this issue as they are running out of storage space. GISC stated that calls are

[16] Automated Fingerprint Information System

retained so they can be reviewed if an issue arises as to data put on Pulse by a call handler.

The Team recommended to GISC that it implement an appropriate retention policy for all call recordings. The Team enquired as to the longest or oldest retrospective requirement for a call recording and GISC referred to one request from AGS for a copy of a call made in the case of a member being accused of a fraudulent call which was required by AGS for a court case. GISC clarified that this call recording was downloaded and collected in person by a Garda Sergeant. GISC estimated there was a time lapse of 10 months approximately between the call being recorded and the request being made.

In terms of the current indefinite retention period, AGS outlined its position that due to the sensitive nature of some data captured by GISC and the fact that such data remains on an individual's record indefinitely, it is essential that the voice traffic is retained indefinitely in the event that queries arise concerning the accuracy of the information captured.

Physical Security: Waste Disposal

The Team enquired as to whether GISC had a contract with a third party in terms of waste disposal and GISC outlined that in fact the shredding of all paper waste was completed in house by GISC staff. GISC clarified that the shredded material is then collected by a local company McGrath Industrial Waste Ltd who collect recyclable materials on an annual contract since 2006. AGS also stated that confidential waste is also disposed of by this Company as the need arises but overall GISC stated it considered that very little data from PULSE or any other AGS sources would be handled in printed format and that the majority of data processed was done online via PULSE and over the phone without there being any need to initiate PULSE print outs etc.

Overall, the Team considered that based on the inspection of GISC, its interaction with GISC caller operatives and examination of the procedures for recording data as outlined in the PULSE manual, there were no data protection issues of concern arising with regard to the processing of data in GISC.

5. Non-PULSE Databases

AGS reiterated the point it made at the pre-audit meeting on November 5th that there was also a substantial number of systems and databases sitting outside PULSE. AGS provided the Team with a diagram featuring the various datasets/functions sitting directly within PULSE such as Court Outcomes, Firearms, Property/Property Match, Summons and areas located on the outer perimeters of PULSE such as Driver Licence Insurance Production, Witness Summons, Warrants, Domestic Violence Orders, and Registered Interests. The Team noted the Electoral Register appeared to be appended to PULSE and AGS confirmed that it is included on PULSE but has not been updated since circa 2005. The diagram also featured databases separate but searchable via PULSE such as the Garda Automated Fingerprint Information System (AFIS). The overview diagram also captured external data feeds to and from external agencies such the Courts Service, the NVDF and the C.S.O as well as databases located off PULSE such as the Fixed Charge Processing System (FCPS)

5.1 Sex Offenders Register.

The PULSE architecture diagram featured a number of databases depicted as sitting within AGS but with restricted access such as the Sex Offenders Register.

AGS outlined that the Sex Offenders Management & Intelligence Unit at the National Bureau of Criminal Investigation provides overall management of PULSE records of all persons who are subject to the requirements of the Sex Offenders Act, 2001.This includes garda monitoring of sex offenders post release and ensuring compliance with all requirements such as being required to notify the Garda Síochána within 7 days of their release from prison that they have been convicted of a sex offence and providing their name and address. They must also notify AGS of any change in address or name and must give notice if they intend to leave the State. AGS stated that this Unit has a process in place to ensure that details of individuals who are no longer subject to the requirements of the 2001 Act are updated accordingly. AGS clarified that the periods for which persons are subject to the requirements of Part II of the Sex Offenders Act 2001 are prescribed by section 8 of the Sex Offenders Act 2001 and are imposed automatically in line with the sentence handed down to the offender in Court.

AGS outlined how there is a tiered restricted access to functionality on PULSE relating to persons subject to the Sex Offenders Act 2001. AGS clarified to the Team that most members of AGS cannot access the Sex Offenders Register per se but if conducting a search on PULSE of a person it would be signalled to the garda member that the person was on the Register. AGS outlined that this information needs to be available as the offenders might have to report at a nominated Garda station. All Garda members can create the initial notification for a Sex Offender on PULSE.

Functionality to search for records relating to Sex Offenders on PULSE is restricted to staff attached to the Domestic Violence & Sexual Assault Investigation Unit, nominated Divisional liaison inspectors and other nominated members that are responsible for overseeing or implementing the 2001 Act within their own area of responsibility.

AGS clarified that not all persons convicted of a sexual offence are subject to the 'Requirements of the Sex Offenders Act 2001'. Persons convicted of a sexual offence (as defined in the Sex Offenders Act of 2001) who had completed their sentence prior to the commencement of Part 2 of the Sex Offenders Act 2001 were never subject to the 'Requirements of the Act'.

AGS cited HQ Directive 81/2009 and the Garda Síochána Policy on the Investigation of Sexual Crime, Crimes against Children, Child Welfare 2nd Edition, 2013 as key references providing guidance in relation to the retention and access levels of records regarding Sex Offenders on PULSE.

The Team considered that based on the information supplied by AGS there were no data protection issues arising with regard to the processing of data on the Sex Offenders Register.

5.2 CJIP – Criminal Justice Integration Project

AGS outlined that the successful completion of the Criminal Justice Integration Project (CJIP) led to the provision of an electronic interface between AGS and the

Courts Service, with all District Court outcomes and Circuit Court appeals of convictions in the District Court being electronically relayed by the Courts Service back to AGS since 2008. AGS considered that the success of the integration had led to new efficiencies and to improved accuracy in relation to data held on PULSE.

AGS outlined to the Team that a murder charge would firstly be heard in a District Court and typically the suspect would appear in the District Court and be charged but it was likely that a case such as this would eventually be sent forward for trial to the Central Criminal Court. AGS clarified to the Team that as of yet there was no electronic system for the transmission of details of Circuit/High/Central Criminal Court outcomes by the Courts Service to AGS. AGS agreed that this meant there was an onus on members of AGS attending court hearings to record the outcomes of these cases accurately and comprehensively. In this respect, AGS stated that HQ Directive 109/2011 provides specific instructions relating to the recording of court outcomes. In summary, Case Supervisors are appointed by their District Officer and are responsible for the recording on PULSE of the court outcome in respect of all Trials before the Circuit and Higher Courts. In some instances AGS clarified that the recording of some court outcomes is carried out by civilian staff based in GISC. The Team was informed that Garda members can contact GISC and request the result of Trials conducted before the Circuit and Higher Courts to be recorded on PULSE by GISC staff.

The ODPC recommends that all court outcomes are fed through to PULSE electronically via CJIP so as to ensure the accuracy of information held on PULSE.

It was also clarified to the Team that in terms of court outcomes, a PULSE record contains a record of whether there was a conviction or non-conviction or if the case was struck out. A certified court outcome can only be obtained from the court and if an outcome was appealed the AGS indicated that it might have to go to the Court Service to obtain this certified copy of the court outcome signed by a judge.

5.3 Driver Enquiry/Vehicle Search

The National Vehicle Driver File (NVDF) consists of two separate files: the National Vehicle File (NVF) which holds the registration and ownership details of all vehicles; and the National Driver File (NDF) which provide details of all the licensed drivers in Ireland. (NVDF arises from the original naming conventions where it was proposed that the data would be supplied in a single file by the Department of Transport).

AGS outlined that it receives the NDF file once a week from the Department of Transport (DoT). The file is transferred from the DoT to the AGS Secure Server via the Secure Government VPN and on successful processing of this file, AGS will send an acknowledgement file to DoT.

NVF vehicle record updates received from DoT are applied twice weekly to the records held on the Vehicle table. The NVF file is loaded into the PULSE vehicle table and held with vehicle records created directly from within PULSE (i.e. foreign registration vehicles). The NVF file records held within the PULSE Vehicle Table are ‘read-only’.

AGS clarified that the NVF & NDF files are loaded into and held within the PULSE database as separate tables.

AGS confirmed that if a 'driver enquiry' (as opposed to a person enquiry) is made in PULSE the information is not taken from PULSE itself, the enquiry is actually made against the National Vehicle Driver File (NVDF). AGS demonstrated how a driver could be looked up via PULSE (but actually against the NDF) by either their licence number or by entering their name and date of birth. In this respect, AGS clarified that they do not have audit trails for these look ups as it is the NDF that is being accessed as opposed to PULSE. Where a search for a vehicle is carried out on PULSE, but there is no match for that vehicle, a record is still retained on PULSE of the vehicle searched for and of the member who carried out the search.

AGS clarified that data held on the NVDF does not feed into the 'person' profile within PULSE, so if a person who had never had any dealings with AGS was searched using the person search within PULSE (as opposed to the driver enquiry) then there would be no data returned on that person.

AGS stated that the number of penalty points on a driver's licence cannot be viewed by AGS. AGS are notified when a driver has been disqualified from driving based on accumulating twelve penalty points.

AGS confirmed to the Team that members of An Garda Síochána do not have access to Penalty point data. AGS outlined that this information is not available on PULSE and is compiled by the Road Safety Authority (RSA). An Garda Síochána receives details, from the RSA, of drivers disqualified as a result of having accumulated 12 or more penalty points in any three year period. This information can then be manually entered onto PULSE. AGS clarified that this information is disseminated to the relevant Districts and recorded on PULSE at a local level.

Legislation governing the operation of the penalty point system is covered in the Road Traffic Act, 2002. The RSA maintains a record of an individual's penalty points. A driver will receive a written notification informing them that points will be added to their driving licence record, points are being removed from their record, that they have been disqualified from driving. In general, penalty points remain endorsed on the driver's file for a period of three years. Any driver accumulating 12 or more penalty points within any given three year period will be disqualified from driving for six months. The RSA will notify the individual concerned and will also notify An Garda Síochána of the disqualification and the date from which the disqualification will take effect. An Garda Síochána are only notified by the RSA when the driver is to be disqualified.
The 'Driver Lookup' functionality on PULSE does not list the number of penalty points associated with a driving licence record. While a driver may receive penalty points as a result of a conviction for a penalty point offence, this information will not be displayed in the Court Outcome details on PULSE. The RSA should be notified of the conviction by the Courts Service and the RSA will be required to collate any other points issued or disqualifications resulting from any single occurrence. The RSA will be aware of the date these points, if any, take effect and the number of points that are actually being added to an individual's record.

AGS confirmed that the details of any disqualification imposed in court resulting from the prosecution of an offence will be recorded in the court outcome and will be visible on PULSE (e.g. details of a consequential or ancillary disqualification imposed in the District Court will be included in the Court Outcome created as a result of receiving the information electronically from the Courts Service).

The Team enquired regarding the terms of the mutual recognition of driving disqualifications between Ireland and the UK (including Northern Ireland) which came

into operation from 28 January 2010. The Team queried whether the AGS received this data from the RSA or the UK police force. AGS indicated in response that it does not have a role in the mutual recognition of disqualifications.

In support of the assertion that the number of penalty points on a licence was not visible in PULSE (bar when the number accrued was 12), AGS demonstrated to the Team that an individual who had for example incurred 6 penalty points would not even appear on PULSE in these circumstances unless a fine arising from a fixed charge e.g. speeding was not paid and a summons issued. The Team noted that the Fixed Charge Processing System was situated outside PULSE as per the PULSE architectural diagram.

AGS stated that the Fixed Charge Processing System (FCPS) is a national computerised system specifically designed to process Fixed Charged Notices (FCN). The Fixed Charged Processing Office (FCPO) is located in Thurles and is operated under the auspices of the Garda National Traffic Bureau (GNTB). The FCPO is predominantly staffed by civilians who input the Fixed Charge Notice details on the FCPS. AGS clarified that only unpaid fines were transferred from the Fixed Charge Processing System over to PULSE to facilitate prosecution.

AGS clarified to the Team that FCPS incidents can be 'Intercept' (E.g. Driver stopped on street by Garda) or 'Non-Intercept' (E.g. Car parked on double yellow lines or caught on speed camera) offences. In other words, the Garda interacts with the driver and records the driver's details (e.g. Name, address and date of birth) or the Garda does not interact with the driver and the vehicle registration number is recorded which FCPS uses to retrieve the owner details recorded on the National Vehicle File (NVF). The NVF does not include a date of birth for the owner of the vehicle.

AGS Donnybrook outlined to the Team the importance of the Fixed Charged Processing Office (FCPO) tagging fines to the correct station and area and made reference to the importance of ensuring the fine has been assigned to the right person, for example, where two persons of the same name reside in the same dwelling. AGS outlined to the Team the steps required in order to ensure the correct assignation of the fine to an individual as follows:.

> "The details recorded on warrants received from the courts service for the non payment of fines, issued as a result of an FCPS incident, will be based on the information that was submitted to the Courts Service. This information will vary, as outlined above, depending on whether the FCPS incident was an 'Intercept' or a 'Non-Intercept' offence and on whether the incident on PULSE was manually created or automatically created by FCPS. Incidents created automatically by FCPS will not contain a local station for the person record. Non-Intercept incidents will not contain a DOB for the person record as this information is not available from the NVF. FCPS will create a new person record on PULSE, based on the available information, where it is not possible to identify a match. Where two persons with the same name reside at the same address (e.g. father and son) it will be necessary for the member attempting to execute the warrant to carry out the necessary enquiries in an effort to establish to whom the warrant refers (e.g. who is the car registered to or who was driving the car at the time of the incident)."

Where the Fixed Charge Notice, is not paid, FCPS will create an incident on PULSE and create a summons application which will be forwarded electronically to the courts service using the available information. AGS clarified that if it was a 'Non-Intercept'

offence, then the summons application submitted to the Courts Service will not contain a date of birth nor will the driver's 'Local Garda Station' be recorded either.

AGS clarified to the Team that Driving Licence and Insurance Production (DLIP) functionality was introduced as part of PULSE Release 2. DLIP records are created on PULSE and will create a link between the DLIP record, the Person record and the Vehicle record. However, the Catalogue screen was designed to only display 'Major entities' and does not display a DLIP record on the catalogue screen. (A sex offender notification that is recorded against the person record is not displayed on the Catalogue screen either). FCPS incidents can be accessed via PULSE but are not a core part of PULSE functionality and therefore would not be displayed on the person's catalogue screen.

AGS stated that some enquiries made on a person or vehicle that did not include a reason for checking the record could be as a result of a DLIP record being created on PULSE which may not be evident through the Persons or Vehicle's Catalogue screen in PULSE.

The ODPC considered that based on the information supplied by AGS there were no data protection issues arising with regard to its examination of this area.

5.4 Prisoner Information Exchange

AGS clarified that there was currently no data feed directly into PULSE from the Irish Prison Service regarding the details of prisoners in custody/ released in Irish prisons. AGS outlined that a notification of 'Prisoner Committals' and of 'Prisoner Releases' is sent to An Garda Síochána by the Prison Service two to three times a week. This information is sent by the Prison Service via the Government Services on a dedicated encrypted VPN tunnel. The data sent via this tunnel is encrypted using software. This notification is disseminated to Criminal Intelligence Officers, District and Divisional Officers nationwide.

The Team enquired whether this data was incorporated onto any restricted area of PULSE or available generally within PULSE e.g. would the date of committal/release of a prisoner be tied into PULSE and evident in a person search for example.

AGS outlined in response that there is no direct electronic interoperable system between the Irish Prison Service and An Garda Síochána's Information Systems. Notifications relating to Prisoner Releases / Committals are disseminated via e-mail to Divisional Offices, District Offices and Criminal Intelligence Officers (CIO). The CIO can manually create an intelligence record on the PULSE system to record specific details relating to an individual or can disseminate the information of an impending release locally.

In addition, the 'Prison Prisoner List' is a stand alone web application available on Gardaís' PCs which allow AGS to establish if an individual is on the Prison Prisoner List. The information is supplied by the Irish Prisons Service and is not linked or integrated with PULSE.

6. Fingerprinting & Photographs

Fingerprints and photographs constitute particular categories of personal data. They are also central to police investigative activity. The Team therefore examined the

circumstances in which such personal data was processed by AGS. AGS stated that the primary legal basis under which photographs, fingerprints and palm prints are taken is section 6 of the Criminal justice Act 1984 as amended by the Criminal Justice Act 2007.

The Team met with AGS in the Garda Technical Bureau on November 8th, 2012 in order to examine the circumstances under which fingerprints are taken by AGS and subsequently sent for analysis to the Garda Technical Bureau in Garda HQ.

AGS outlined to the Team that under Section 48 of the Criminal Justice Act, 2007 the authorisation to take a photograph, fingerprints and palm prints from a person detained may be granted by a member of An Garda Síochána not below the rank of Inspector. In general photograph, fingerprints and palm prints are taken amicably when an authorisation is granted.

The Criminal Justice Act, 2007 also provides for the use of reasonable force in certain circumstances. A member of An Garda Síochána may, where a person is detained under section 4, and he or she fails or refuses to allow his or her photograph or fingerprints and palm prints to be taken pursuant to section 6, use such force as he or she reasonably considers to be necessary to take the photograph or fingerprints and palm prints. AGS clarified that such a power shall not be exercised except on the authority of a member of the Garda Síochána not below the rank of Superintendent. Photographs or fingerprints and palm prints taken pursuant to this section shall be taken in the presence of a member of the Garda Síochána not below the rank of Inspector. In these circumstances, the taking of such photographs and fingerprints and palm prints shall be video-recorded.

The Team examined the provisions of the Criminal Justice Act 2007 in relation to fingerprints and noted the provision in section 48 (b) of the 2007 Act amending the Criminal Justice Act 1984 to allow for “use of reasonable force in certain circumstances”.

> 6A.—(1) Without prejudice to the generality of section 6, a member of the Garda Síochána may, where—
>
> (a) a person is detained under section 4, and
> (b) he or she fails or refuses to allow his or her photograph or fingerprints and palm prints to be taken pursuant to section 6, use such force as he or she reasonably considers to be necessary to take the photograph or fingerprints and palm prints.

The Team also noted that section 48 of the 2007 Act amended section 6 of the Criminal Justice Act 1984 to provide that

> (5) The taking of such photographs and fingerprints and palm prints shall be video-recorded.”,

The Team enquired as to the operation of this provision and was informed that this was a rarely used provision, as this would mean the individual had resisted the taking of prints where reasonable force had been invoked. Theoretically, AGS stated that if it were required to record the taking of prints in this situation, they would likely have 'wet prints'[17] taken in the interview room and have the taking of the fingerprints recorded using the interview recording equipment.

[17] fingerprints taken using ink that are recorded on a paper card template

AGS outlined to the Team that in many cases fingerprints may be taken in order to match or eliminate fingerprints taken at the scene of a crime or serious incident and a record of these might only be held in the Investigations file at the relevant Garda station and these fingerprints will never be uploaded onto the Garda Automated Fingerprinting Information System (AFIS).

The AGS clarified to the Team that all fingerprints taken of individuals arrested and detained will be sent to the Garda Technical Bureau for further examination and comparison and these fingerprints will be uploaded and retained by AGS on AFIS, including those of an individual who is ultimately not charged with any offence.

AGS referred to article 18 of the treatment of persons in custody regulations and stated that if fingerprints were given with the consent of the data subject they must sign a written consent.

The Team subsequently examined these procedures as part of its inspection of Mullingar and Donnybrook Garda stations:

6.1 Photographs/Fingerprinting in Mullingar Garda Station

Photographs

The Team was provided with a **PCO2** form in Mullingar which it noted was a consent form for photographs to be taken.

On the day of the Inspection, AGS also provided the Team with a copy of **Form C72** which is headed Information for Persons in Custody - Regulation 8 of the Criminal Justice Act 1984 (Treatment of Persons in Custody in Garda Síochána Stations) Regulations 1987 and 2006.

The Team observed that the C72 form clearly states that AGS may take a person's photo and refusal to do so is an offence, so it queried as to why the PC02 Form supplied by AGS Mullingar had a voluntary section which states "I am not obliged to provide or permit the taking of such photographs".

AGS responded that the C72 Notice of Rights Form informs the individual that refusal to allow their photograph to be taken is an offence where the taking of that photograph has been authorised by a member of An Garda Síochána, not below the rank of Sergeant, for the purpose of assisting with the identification of the person in connection with any proceedings that may be instituted against them for the offence in respect of which they had been arrested. Sec 12 Criminal Justice Act, 2006 refers.

The PC02 Form outlines the circumstances under which the photograph of a person has been taken. This may fall under either statutory authorisation or voluntary consent. It is an offence to refuse a photograph to be taken under a statutory authorisation. The declaration referred to by the ODPC on the PCO2 Form relates to an instance where the photograph is taken on a voluntary basis. AGS outlined that the primary purpose of the PC-02 form is to have the photograph uploaded onto PULSE.

Fingerprints

In advance of the Mullingar inspection, the Team was informed in Garda HQ that

> "if fingerprints were given with the consent of the data subject they must sign a written consent. AGS stated that this form varies across Garda stations but that it was the intention of the AGS to create a generic form."

The Team noted that the PCO2 form provided to the Team in Mullingar AGS referred to consent to be photographed only and that no form was provided to the Team with a reference to fingerprints and consent (whether voluntary or under statutory authorisation).

After the inspection took place, the Team enquired in writing as to what Form was used by Mullingar AGS to capture the written consent of data subjects to have their fingerprints taken. AGS subsequently provided the Team with a form covering consent to allow fingerprints, palm prints and photographs to be taken. The ODPC notes that this form caters for a scenario where the capture of fingerprints/palm prints/photographs is on a voluntary basis. The ODPC was unsure as to why there was a reference to photographs on this form as the PCO2 form already dealt exclusively with the capture of photographs (whether voluntary or under statutory authorisation).

6.2 Photographs/Fingerprinting in Donnybrook Garda Station

Photographs & Fingerprints

AGS Donnybrook referred the Team to section F of the **Custody Sheet** which is headed **F. Status of Arrested/Detained Person** and which then lists 6 possible categories under which the individual might be held

- Section 4 Criminal Justice Act, 1984
- Section 2 Criminal Justice (Drug Trafficking) Act, 1996
- Section 30 Offences against the State Act, 1939, as amended
- Section 50 Criminal Justice Act, 2007
- Section 42 Criminal Justice Act, 1999 as amended
- Other

AGS Donnybrook clarified to the Team that any person arrested or detained outside of the Acts listed above (falling into the category of 'other' above) would not be required to give fingerprints, palm prints or photographs. In these 'other' instances, a data subject might volunteer to give their fingerprints and palm prints. The Team welcomed this clarification and noted that section T of the Custody Record - **'Fingerprints, Palm prints, Photographs** – was also consistent in that the same Acts were cited - where arrested-detained under etc. In addition, the Team noted that the rules governing when fingerprints, palm prints or photographs are required are also reflected in the **C.72. Information for Persons in Custody** form**.** In addition, the C.72. Information for Persons in Custody also states

> "In any other case if you volunteer, a member may take your fingerprints, etc with your written consent and, if you are under eighteen, the written consent of your parent/guardian."

AGS Donnybrook referred the Team to section K of the Custody Sheet which is headed **K. Photograph- Section 12 Criminal Justice Act 2006** and has a yes/no tick box as to whether the individual was photographed. AGS Donnybrook stated a Sergeant can authorise the taking of the photograph and that this section provides for circumstances where the data subject gives their written consent to be photographed.

AGS Donnybrook provided the Team with a copy of its yellow **PC02 Form - Consent for taking of Photographs, Fingerprints and Palm prints**. AGS Donnybrook also provided the Team with another form '**Consent for taking of Photographs, Fingerprints and Palm prints'**. The Team could not discern any substantial differences between the purposes of each form but noted that the second form contained information addressed to the data subject which was not present on the yellow PC02 form. The Team noted the second form supplied by AGS Donnybrook contained a signed statement from the data subject

> I……..D.O.B…….
> of……..
> have been cautioned that I am not obliged to consent to have my photograph, fingerprints and palm prints taken. I understand that if I do consent to the taking of my photographs finger prints and palm prints and the results of any comparisons, examinations or tests on photographs, fingerprints and palm prints taken may be used in evidence.

The Team enquired whether AGS Donnybrook used both forms and if so could they provide an outline of what they considered the key differences to be between the two forms.

AGS Donnybrook clarified that it uses the form PC02 when consent is not given by a prisoner to take his/her photograph voluntarily. AGS reiterated that statutory authority can be invoked to photograph a prisoner under the various sections of legislation as laid out in the PC02. This form is accompanied by the PC65 form which can be used if consent is given to have fingerprints taken or if the statutory authority has to be invoked. In the middle section of the PC65 form, the member has to specify which authority the fingerprints have been taken under or if it has been provided voluntarily.

Overall, in light of both the Mullingar and Donnybrook inspections, the Team noted that whilst the **Custody Record** provides for the taking of the data subject's photograph with their consent, it does not appear to contain any reference to instances where a data subject volunteers to give their fingerprints. The ODPC sought clarification on this point. AGS confirmed that the Custody Record form C.84 4 does **not** provide a specific section to indicate that a data subject volunteered fingerprints. AGS stated that the procedure to record the voluntary provision of fingerprints by an individual in the Custody Record was to enter details in the 'Details of action/occurrence' section of the custody record.

The Team considered that the fingerprinting process duly outlined by AGS Donnybrook should be replicated across AGS.

6.3 Standardised Procedures & Forms

AGS acknowledged that older versions of forms were in use in some Garda districts and should be discontinued. Subsequent to the inspections, AGS HQ supplied the Team with two draft Fingerprint Consent Forms. The Team noted the first form

catered for situations under statutory authorisation where a person is compelled to provide their fingerprint/palm print under section 28 of the Criminal Justice Act 1984. The second form was designed in line with 'regulation 18' of the Criminal Justice Act 1984 (treatment of Persons in Custody in Garda Síochána Stations) Regulations 1987 and 2006 where the data subject signs a statement saying they freely consent to the giving of their fingerprints.

The ODPC considers the introduction of these forms on a generic basis to be used by AGS at all times would ensure consistency and transparency in terms of a data subject being made aware of their rights at the point of capture of their finger prints/palm prints. However, this view is predicated on the addition to these forms of adequate information regarding the right of the data subject to have their fingerprints deleted in certain situations. Overall, it is recommended that generic forms for fingerprinting, palm prints and photographs should be designed, signed off and circulated by AGS as soon as possible for universal use to ensure consistency.

If fingerprints are taken, AGS stated that a notice of rights would be issued as per the information on Fingerprints, Palm Prints, Photographs and Tests contained in **C.72. Information for Persons in Custody.** The Team queried as to whether the notice of rights was in accordance with regulations 8(1) and 8(2) of the Criminal Justice Act, 1984 (Treatment of Persons in Custody) Regulations 1987 and 2006 namely 8(2) which provided

> (2) The member in charge shall without delay give the arrested person or cause him to be given a notice containing the information specified in subparagraphs (b) and (c) of paragraph (1) and such other information as the Commissioner of the Garda Síochána, with the approval of the Minister for Justice, may from time to time direct.

AGS outlined its position that the **C72. Information for Persons in Custody** is the written notice given to prisoners outlining all the rights of a prisoner while in Garda custody in accordance with Regulation 8(1) and 8(2) of the Criminal Justice Act, 1984 (Treatment of Persons in Custody) Regulations 1987 and 2006. AGS also indicated there are numerous additional written notices relating to persons in custody e.g. Electronic Recording of Interview notices, Suspension of Questioning form, Notification to Drunk Driver in relation to specimens etc.

The ODPC considers that the C.72 written notice is in accordance with the regulations but in situations where fingerprints or palm prints are captured it considers that additional information regarding an individual's rights to information regarding the retention of their fingerprints and associated rights is required to be provided in writing at the time of capture (see section 6.6. below).

AGS referred to a Working Group on Fingerprints within AGS which was reviewing a number of the matters arising in this area. AGS stated that a revised fingerprint policy had been drafted and sent to the Garda Commissioner for approval. AGS clarified that this new policy was internal AGS policy and that its main focus was to ensure the correct handling of evidence and further action taken at all times on foot of positive fingerprint identifications.

AGS also indicated it intended to draft a separate form for photographs as some of the existing forms cover photographs/fingerprints/palm prints. Since the inspection, AGS informed the Team that a revised PC-02 form, designed to deal with photographs only, was created and the current version of this form was added in December 2012 to the list of forms that are available on AGS portal. The primary

purpose of the PC-02 form is to have the photograph uploaded onto PULSE. This form records details of the person and photograph, the authority for the taking of the photograph (includes voluntary photographs), the officer that authorised the uploading of the photograph onto PULSE and details of the CIO that added the photograph onto PULSE.

6.4 Livescan

AGS stated that in many instances fingerprints are taken using what are known as Livescan - electronic fingerprinting machines which take fingerprint and palm print scans on a large scanner- which transmit the prints directly into AFIS. AGS clarified that there are 24 Garda stations around the country equipped with Livescan machines. The AGS also clarified that both palm and fingerprints are taken at the same time. AGS stated that where prints are taken not using Livescan, the prints are hand delivered to the GTB and that each Garda district has a day allocated for delivery of prints to the Technical Bureau.

In terms of the requirement for persons applying for asylum in Ireland to be fingerprinted, AGS outlined that some Garda stations such as Leixlip are set up in such a way that they provide a joint Garda National Immigration Bureau/criminal fingerprinting area. All fingerprinting for Garda National Immigration Bureau purposes is done by members of AGS working as immigration officers for the Garda National Immigration Bureau.

The Team viewed the Livescan printer used by the AGS for fingerprinting purposes in Mullingar. The Team also visited the office of the GNIB officer. The Team enquired whether the Livescan fingerprinting equipment was dual purpose i.e. whether Mullingar AGS take fingerprints for both criminal investigation purposes and immigration/GNIB purposes. AGS Mullingar confirmed the Livescan printer was dual purpose and used by the GNIB officer.

6.5 Fingerprinting Service for Visa Applications abroad

AGS Donnybrook informed the Team that it provides sets of fingerprints to individuals who are required to supply them to countries they intend to visit as part of their visa application. AGS Donnybrook confirmed they do not retain any record of the fingerprints and the only documentation with regard to this service is the recording on the Garda accounts of a note of the taking of the fingerprints, the date and the amount received. AGS clarified that the taking of fingerprints in these circumstances is a service provided nationally by AGS. AGS indicated that the fee (currently 60 euro) associated with the provision of this service generates revenue for the exchequer. HQ Directive 107/2011 - 'Revised Fees Charged by An Garda Síochána' refers.

6.6 AFIS (Automated Fingerprinting Information System)

The Team visited the Garda National Technical Bureau to examine the work of the fingerprint section which is the largest section in the Technical Bureau. The fingerprint section has a staff of 46 comprising an Inspector, 9 Sergeants, 30 Gardaí and 6 civilians.

The Team was provided with access to the Garda Automated Fingerprinting Information System (referred to hereafter as (AFIS). AGS provided the Team with the

table below which contains the total number of Tenprint cases submitted to the Automated Fingerprinting Information System (AFIS) system as of the 31st July 2013.

Tenprints on System (as of 31st July 2013)

Record Type	Total Number on Database	6 Month Period Feb to July 2013
GNIB	84,445	20,900
Criminal	375,540	7,669
eVisa	15,035	2,455
ORAC	27,048	423
Interpol	5,734	1,198

In relation to the figures above, AGS clarified that ORAC relates to fingerprints taken by the Office of the Refugee Applications Commissioner (ORAC) of asylum seekers. GNIB and eVisa refer to fingerprints taken for Immigration purposes, for example, the Garda National Immigration Bureau (GNIB) take fingerprints of all non-EU nationals on registration in the state.

Note: Criminal total includes all livescan, legacy, wetink and prison submissions
ORAC total includes all livescan, wetink and asylum legacy submissions

AGS informed the Team that in total there were 507,802 sets of fingerprints stored on the AFIS system as of the 31st July 2013.

Fingerprints of Asylum Seekers and Non-Nationals

The Team noted that scanned fingerprints taken for asylum and immigration purposes are retained within AFIS. The Team also noted based on a previous audit of ORAC that the asylum prints are scanned into EURODAC[18] using an interface with AFIS. Up until the inspection the Team indicated to AGS that it was not aware of the full extent of the volume of fingerprints being captured in the non-criminal context.

AGS confirmed to the Team that the fingerprints of asylum applicants are examined for possible matches if AFIS is searched by AGS for criminal investigation purposes. The Team viewed records of asylum applicants appearing in searches conducted by GTB staff to assist them in the identification of fingerprints. AGS stated to the Team its view that although asylum applicants fingerprints were retrievable if AFIS is searched by AGS for criminal investigation purposes, it considered there was a logical separation between fingerprints held in AFIS for asylum/immigration purposes to fingerprints held on AFIS for criminal investigation purposes.

[18] EURODAC is a central database used to store fingerprints of individuals who have applied for asylum in an EU Member State. It is used to identify individuals who may have made previous asylum applications.

We referred AGS to "purpose limitation" a key concept and principle in data protection legislation where the purpose of any processing of personal data is clearly restricted to a specific purpose(s) and must not lead to any personal data gathered in one context, being used for another unrelated or unspecified purpose. Regarding the fingerprinting of individuals for asylum and immigration purposes, the ODPC would not have expected that a search conducted on the AFIS criminal finger prints database would lead to the records of applicants for asylum appearing in the search results. We indicated to AGS our understanding in advance of the audit that these areas were kept completely separate and was assured of this in the course of its audit of GNIB in March 2011.

Excerpt from GNIB Audit of March 2011:

> It was clarified to the Team by GNIB that the prints taken are not retained on the 'core' AFIS system which is a criminal fingerprint database but rather they are stored on a separate area of 'AFIS'.

This Office considers that although these datasets may well be designated as 'separate' in reality these datasets are integrated when searches are conducted on AFIS for criminal investigation purposes. This negates the idea of there being any real separation. The current structure is likely to lead to the details of all individuals who presented themselves in an asylum or immigration context being included (without their knowledge or consent) in fingerprint searches conducted as part of criminal investigations.

We also refer to media analysis of AFIS and note the same understanding

> The AFIS database was announced in November 2006, with a completion period of 18 months. It is held in the Garda Technical Bureau at Garda Headquarters, at a cost of €18 million. It was modelled on the system used by the FBI in the US, and Ireland was one of the first EU countries to introduce it.
>
> It replaced the Technical Bureau's central fingerprinting system – which held fingerprints from crime scenes and suspected criminals – and upgraded the fingerprinting facilities in the Office of the Refugee Applications Commissioner (ORAC) for asylum seekers.
>
> In relation to ORAC, the system allowed the Garda National Immigration Bureau to take fingerprints of all non-EU nationals on registration in the state. **These are kept separate from criminal fingerprints for data protection and civil liberty reasons.**[19]

AGS responded stating that

> "the decision to search crime scene fingermark [sic] to the entire database including GNIB and Asylum is necessary and the opinion of the Attorney General is that it is correct to do so and may be seen as a failure of duty not to do so".

We requested that AGS clarify whether there is any legal basis or provision in the criminal justice acts or immigration law allowing for the processing of fingerprints of asylum seekers and non-nationals entering the country for criminal investigation purposes.

[19] http://www.irishexaminer.com/text/ireland/kfkfaugbgbkf/

The Garda National Immigration Bureau provided the following response:

"*An Garda Síochána undertakes three (3) particular functions of relevance with regard to the immigration process which is operated in the State. Firstly, members of the Garda Síochána who have been appointed as immigration officers by the Minister for Justice and Equality, pursuant to section 3 of Immigration Act 2004, undertake immigration controls at approved ports of entry to the State. Secondly, a requirement is placed on An Garda Síochána, at section 9 of the Act of 2004, to maintain a register of particular non-nationals who are resident in the State. Thirdly, the Garda Síochána also engages in the process of removing non-nationals from the State in circumstances where they no longer have permission to remain here.*

Section 9 of the Act of 2004 requires a non-national to furnish certain particulars to a registration officer for the registration district in which he or she is resident. The list of these particulars is set out at in Schedule 2 of the Act. Paragraph II of the Schedule requires provision of "signature and fingerprints if required by the registration officer.

An immigration officer may, on behalf of the Minister for Justice & Equality, pursuant to the provisions of section 4(3) of the Act of 2004, refuse to give a non-national "a permission" if he/she is satisfied, among other things, "that the non-national has been convicted (whether in the State or elsewhere) of an offence that may be punished under the law of the place of conviction by imprisonment for a period of one year or by a more severe penalty" or "that the non-nationals entry into, or presence in the State could pose a threat to national security or be contrary to public policy".

Thus, the main purpose for taking fingerprints in the process of registration of non-nationals provided for at section 9 of the Act of 2004, is to ensure that a permission to land or reside in the State is not given to a non-national in circumstances where he/she has a criminal conviction or is suspected to have been involved in criminal activity.

It is important, also, where a non-national has been granted a permission to reside in the State and subsequently acquires a criminal conviction or engages in any activity which could pose a threat to national security or be contrary to public policy, consideration is given, as soon as is possible, to revoking the said permission. The capacity of the Garda Síochána to fulfil its responsibilities regarding the granting/refusal of permission to land/reside in the State to non-nationals is significantly enhanced through the taking of fingerprints in the process of registration of non-nationals.

With regard to fingerprints provided by non-nationals who make an application pursuant to the provisions of the Refugee Act 1996, this is a matter which falls within the remit of the Office of the Refugee Applications Commissioner (ORAC). Non-nationals who arrive in the State and make an application pursuant to the Refugee Act,1996 are fingerprinted pursuant to the provisions of that Act and are issued with a 'temporary residence certificate'. As previously stated, non-nationals who are granted a permission to remain in the State for a period of longer than ninety (90) days are required to register with an Garda Síochána and are fingerprinted in that process in advance of being issued with a 'registration certificate'.

It appears reasonable for the reasons outlined above, that fingerprints provided by non-nationals who are placed on the register of non-nationals are matched against the criminal database. This is to ensure that that they do not have a criminal record or are suspected to pose a threat to national security.

It is also relevant to mention, that the vast majority of applications for asylum are rejected, possibly in excess of 90% of the total. Therefore, if asylum applicants were not required to provide fingerprints and those fingerprints were not matched against other databases, the making of an asylum application would provide a mechanism for persons with criminal intent or who pose a threat to the State, to avoid being detected. The extent to which bogus identifications and otherwise false information is provided in the asylum process has resulted in GNIB establishing a particular operation targeting the criminality involved.

The following is an example of the importance of using fingerprints in tackling the aforementioned issues. On a particular day a non-national who had first arrived in the State as an asylum seeker presented at the registration office operated by GNIB at Burgh Quay, Dublin, 2. Due to uncertainty which arose regarding his true identity, his fingerprints were taken. On checking the said fingerprints with relevant databases it was revealed that the man was known to the UK immigration authorities by another identity and had been involved in criminal activity in the UK. It was also revealed that the man while known by another identity was one of the most wanted people in Europe, due to his suspected involvement in the trafficking of up to one hundred children to Europe from Africa, for sexual exploitation. This man was subsequently extradited to The Netherlands, where last year he stood trial and was convicted of offences relating to human trafficking, where the victims were children who were to be sexually exploited.

In, addition, under Section 15 of the Irish Nationality and Citizenship Act, 1956 the Minister must be satisfied, amongst other conditions, that an applicant for citizenship 'be of good character' to grant an application for citizenship."

AGS outlined that the Core AFIS database is partitioned to store asylum applicants' fingerprints and fingerprints captured as part of criminal investigations in separate logical partitions on the AFIS database. The AFIS solution provides the ability to define the target database to be searched when submitting a search. This is defined at the workflow level and is a business rule for all searches carried out using a particular workflow. AGS stated that the system workflows and business rules were defined as part of the requirements sessions held in 2006 for the new AFIS system. The system workflow for criminal tenprint searches is designed so that the search will be preformed against all tenprints including those stored in the asylum seeker partitions of the database.
AGS further outlined that searches on the AFIS database base conducted for criminal investigation or as part of the registration of non-nationals are carried out across all records on AFIS, including 'Criminal', GNIB, ORAC, eVisa and Interpol records. The source of the records of any matches found will be returned as part of the search results.

AGS reiterated its view that based on advice from the Office of the Attorney General, fingerprints and related biographical data of asylum seekers taken after the commencement of the Immigration Act, 2003 can be shared in full with An Garda Siochana. AGS stated that advice from the Office of the Attorney General has consistently supported the sharing of this information, citing the case of Desmond V Glackin (No. 2) [1993] 3IR 67 and has also advised that the taking of fingerprints under Section 9(A) of the Refugee Act, 1996 (as amended) does not prevent the Gardaí from having lawful access to such fingerprints for the purpose of investigation of criminal offences. AGS recommended that the ODPC reconsider its recommendation on foot of the advice of the Attorney General.

In terms of the legal basis cited by AGS and the Office of the Attorney General, section 9A(6) of the Refugee Act 1996 provides that the Garda Commissioner shall arrange for the maintenance of a record of fingerprints taken under S.9.A(1). In addition, the Immigration Acts 2003 and 2004 require that a permission to land or reside in the State is not given to a non-national in circumstances where he/she has a criminal conviction or is suspected of having been involved in criminal activity. Provision must also be made to allow AGS to revoke any permission granted on the basis of information regarding subsequent criminal convictions coming to light.

This Office does not have an issue per se with the fingerprints provided by individuals who are placed on the register of non-nationals being subject to a search against the criminal database in order to fulfill the requirements of the legislation cited above governing immigration and residence. We do not oppose advice received by the Department of Justice & Equality from the Attorney General in 2002 that although fingerprints can only be taken for "the purposes of this Act" as stated in section 9A of the Refugee Act, "this does not prevent the Gardaí from having lawful access to such fingerprints for the purpose of investigation of criminal offences".

The Office of the Data Protection Commissioner has never considered AGS are precluded from having lawful access to such fingerprints for the purpose of investigation of criminal offences. AGS may invoke section 8 (b) of the Data Protection Acts[20] which provides for access to such fingerprints, but only on a case-by case basis where there is reason to do so. However, it is the view of our Office that Section 8(b) of the Acts would not allow AGS unjustifiable access to this data as the fingerprints have not originally been gathered for law enforcement reasons. Such actions widen the whole basis for the processing of these fingerprints and are in our view incompatible with data protection legislation namely - section 2(1)(c)(i) of the Data Protection Acts - "the data shall have been obtained only for one or more specified explicit and legitimate purposes."

In conclusion, we consider that the integration of the fingerprints of asylum, visa and residence applicants with fingerprints taken for criminal investigation purposes as part of all routine searches performed on AFIS raises issues of concern from a data protection perspective. It is recommended that AGS revisit this issue with the Attorney General in the interests of clarity for all parties concerned taking account of the European legislative context.

In addition to the current situation, we view the imminent introduction of new legislation with regard to the capture of fingerprints and DNA samples for criminal investigation potentially affords greater rights and protection to individuals suspected of a crime than asylum seekers and non-nationals entering the state.

In terms of the legal requirement to delete fingerprints taken for asylum purposes held after ten years, AGS demonstrated the process to the Team which AGS clarified is also subject to review by ORAC in advance of the annual deletion process. AGS stated that ORAC reviews the list of individuals whose records are scheduled for deletion and will revert to AGS with any exceptions. AGS stated it deletes data in batches of 20 and added that it also deletes details of naturalised persons based on lists supplied by ORAC. AGS indicated that it keeps a physical log of all data deleted

[20] Section 8(b) "required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid"

on a register. The Team viewed the physical register of deletions which it noted dates back twenty-five years. The Team considered all to be in order. However subsequent to the inspection, the Team established after further enquiry that when fingerprints are deleted they are not in fact deleted from the back-up tapes but AGS clarified that the fingerprints would not be searchable. AGS clarified that the AFIS back-up tapes are rotated over a five week period and the data contained on any of the AFIS back-up tapes is only available for a five week period before being over-written.

AGS also clarified that a "records that have already expired" report is generated on a monthly basis which would highlight any cases that had been incorrectly restored from a backup. In addition, these issues would only become relevant in the event of a Full Restore being required on the system. Since the installation of the current system in 2007 a Full Restore has never been required.

Visa Applicants

The Team also requested clarification from AGS whether fingerprints being captured as part of the visa application process (e.g. in Nigeria) are also being stored and searched on AFIS. The following information on the INIS website indicated[21] that this was the case:

FAQ

> Collection of biometric data will commence in Nigeria in March 2010 and is likely to be rolled out in other locations at a later date.
>
> **Q10. What will you do with my fingerprint records?**
>
> Your fingerprints will be stored on a central official database in Ireland and will be checked against all records held on this database. In some cases it may be necessary for you to return to the VAC to have your prints retaken before a decision can be made on your visa application.
>
> **Q13. Who will my fingerprint records be shared with?**
>
> Your fingerprint records, and the results of any database searches, may be disclosed to other Irish Government Departments and/or Agencies, including An Garda Síochána (Irish Police), as well as to public authorities of the European Union/EEA, and/or other States, including for the purpose of identification and/or immigration history.

AGS confirmed to the Team that all sets of fingerprints taken as part of the E-Visa (Nigeria) Program are stored on AFIS and are searched against the criminal database.

Prisoners Fingerprints

The ODPC also noted that the fingerprints of all convicted prisoners are also captured and stored on AFIS indefinitely. AGS stated that the fingerprints of prisoners are taken as they begin their sentence and these fingerprints serve as evidence of the conviction and the identity of the person serving the sentence for that conviction.

[21] http://www.inis.gov.ie/en/INIS/Pages/Biometrics%20(Fingerprinting)#10

The Team enquired as to the legal basis for the taking of the fingerprints of prisoners and AGS referred to S.I. No. 252/2007 - Prison Rules, 2007

> **10.**
> (1) The Governor may take and record, or cause to be taken and recorded, measurements, photographs, fingerprints and palm prints of a prisoner at any time during the period of his or her imprisonment.
>
> (2) The Governor may provide or cause to be provided to the Garda Síochána, the measurements, photographs, fingerprints or palm prints of a prisoner upon lawful application by a member of the Garda Síochána.

It is the intention of the Office to examine this issue in further detail with both AGS and the Irish Prison Service going forward.

Fingerprints taken for Criminal Investigation Purposes

The AGS referred to subsequent legislative amendments concerning fingerprints in the Criminal Justice Acts of 2006 and 2007. AGS clarified to the Team that the amendments extended the period under which the fingerprints of people taken for criminal investigation purposes could be held by AGS from 12 months to indefinitely unless the data subject themselves requests the deletion of their fingerprints from the Garda Commissioner.

The ODPC examined the provision contained in section 49 of the Criminal Justice Act 2007.

> **Destruction of Records**[22].
> **49.—** The Act of 1984 is amended by the substitution of the following section for section 8:
>
> "8.— (1) Where a person (in this section referred to as 'the requester') has had records taken in pursuance of powers conferred by section 6 or 6A of this Act or section 12 of the Act of 2006, and proceedings for an offence to which section 4 applies—
>
> (a) are not instituted against the requester within the period of twelve months from the date of the taking of the records, and the failure to institute such proceedings within that period is not due to the fact that he or she has absconded or cannot be found, or
> (b) have been so instituted and—
>
> (i) the requester is acquitted,
>
> (ii) the charge against the requester in respect of the offence concerned is dismissed under section 4E of the Criminal Procedure Act 1967 , or
>
> (iii) the proceedings are discontinued,
>
> he or she may request the Commissioner to have the records concerned destroyed or their use limited.

[22] records ' means a photograph (including a negative), fingerprints and palm prints taken in pursuance of the powers conferred by section 6 or 6A of this Act or section 12 of the Act of 2006 and every copy and related record thereof

We ascertained from this provision that if proceedings are dropped or they proceed and the person concerned is acquitted the data subject must write to the Garda Commissioner to apply to have the pertinent records e.g. fingerprints destroyed and if the request is refused the data subject also has the right to appeal this decision to the Circuit Court.

We recommend that the right of application to delete fingerprints held on AFIS for criminal investigation purposes should be added to all the written consent forms signed by persons who either voluntarily provide fingerprints or are compelled by AGS to be fingerprinted as otherwise there seems to be very little awareness made of this right.

We also refer AGS to the "Marper case" where the European Court of Human Rights ruled that the indefinite retention by the UK police of both DNA data and fingerprints was ruled a breach of the ECHR's provisions on privacy. In addition, the recent case of R (on the Application of RMC and FJ) v Commissioner of Police of the Metropolis and Others (RMC and FJ) – 22 June 2012, the High Court of England and Wales held that the indefinite retention of photographs of persons who are arrested but not subsequently prosecuted, breaches the right to private life protected in article 8 of the European Convention on Human Rights.

This Office is aware that the provisions around the retention and destruction of DNA samples and fingerprints are set to change under legislation currently before the Oireachtas[23]. We intend to review this area as soon as the legislation is enacted and destruction schedules commence.

7. Automatic Number Plate Recognition (ANPR)

Automatic Number Plate Recognition (ANPR) is a technology deployed and used by An Garda Síochána's Garda Traffic Corps vehicles to assist them in road traffic enforcement and in specified circumstances the general prevention and detection of serious crime. Currently, there are 108 vehicles fitted with ANPR across the country**.** ANPR vehicles are now deployed in every Garda Division, with the number of vehicles allocated in each division based on various criteria including the type of roads, the amount of motorways and geographic profile.

The Team noted in the first instance that AGS had engaged with the ODPC in advance of the deployment of ANPR.
AGS outlined to the Team that an ANPR system includes an in-vehicle screen, forward facing camera, an IR rear camera, a keyboard and an Ethernet cable with hardware and software in the boot of the vehicle. ANPR systems fitted in road policing vehicles also include a video recording and speed detection facility.

If an ANPR device is installed in a Garda patrol car, the device will take an in-car camera reading, using Optical Character Recognition Technology of the Vehicle Registration Numbers (VRNs) of other vehicles on the road. Each VRN is checked against a database of watch lists. If a 'hit' is detected then an audible signal is given to the members in the vehicle and a picture of the vehicle, its VRN and other relevant information are displayed on the in-car camera screen to enable members of the

[23] Criminal Justice (Forensic Evidence and DNA Database System) Bill 2013 – http://www.oireachtas.ie/documents/bills28/bills/2013/9313/b9313d.pdf

Garda Síochána to make an informed decision about stopping the vehicle in question.

The Team noted that the ODPC was previously advised by AGS that the legal basis relied upon for the deployment of ANPR could be found in the general functions of AGS as set out in Section 7 of the 2005 Garda Síochána Act.

The ODPC was also informed that datasets stored in the ANPR system are made up of the following:

1. Stolen Vehicles,
2. Un-authorised Takings,
3. Untaxed Vehicles,
4. Warning Lists (cars of interest – these are fed into the system by criminal intelligence officers).
5. Uninsured Vehicles.

On the day of the inspection of ANPR procedures, AGS provided the Team with a copy of an ANPR Vehicle Capture Exhibit and a National ANPR Search Request Form. The Team noted that the Request Form allows a member to request details of any sightings of a specific vehicle by ANPR by completing the form outlining the reason for the request and noting the PULSE I.D.

The Team clarified with AGS that AGS do not maintain separate ANPR vehicle warnings and that a PULSE vehicle warning is actually the same as an ANPR warning. In fact, AGS indicated that it would not refer to these warnings as ANPR warnings but PULSE vehicle warnings.

In terms of external data flows, AGS confirmed that with regard to untaxed vehicles, it receives a data feed from the Department of Transport and similarly, a data feed from the Irish Insurance Federation (IFI) in relation to uninsured vehicles.

AGS stated that fifteen individuals are authorised to access the ANPR database and of these 15, 11 were active users including three officers drawn from the Garda IT division– administrators of the system, two officers from the Garda Síochána Analysis Service – who use the database for analysis only, three officers attached to GNTB to interrogate the system for National Investigations and 3 officers from Crime and Security Division who have access to the database to conduct sensitive searches.

The Team viewed a sample of recent ANPR requests and sought to confirm that retention was in line with that previously notified to the Office. The Team noted one of the requests was in relation to a recent high-profile disappearance and also noted requests that were declined by ANPR division as they did not meet the requirements to warrant using ANPR. In this respect, AGS clarified that each application to interrogate the ANPR database must meet requirements such as Pulse ID, how the vehicle is relevant to the investigation. It must be approved and forwarded by the Senior Investigating Officer, etc.

In terms of the live system, it was established that only 90 days of records are searchable in response to requests from Garda Divisions. As to the retention period for data stored on the ANPR system, AGS clarified that the retention period is 90 days but that data is also segregated in such a way that the system can only be searched beyond that period in relation to serious crime investigations. These

searches must be performed with the approval of the Chief Superintendent of Crime and Security.

AGS further outlined that data entered in relation to serious crime can be searched but that it was not possible to view back beyond a year. AGS confirmed that the "seen" data captured by ANPR vehicles is retained on the ANPR database for 365 days. After 365 days the system automatically deletes this information. Only registrations and date relating to vehicles of interest is retained on the system after this period.

The Team considered that based on the information supplied by AGS there were no data protection issues arising with regard to the processing of data using ANPR.

8. Access to Telecommunications Data

The Team met with AGS Crime & Security Division which is headed up by Assistant Commissioner John O'Mahony. The Team outlined to AGS its intention to focus on requests for communications data made by Crime & Security Division, primarily under the provisions of the Communications (Retention of Data) Act 2011. The purpose was to establish procedures and compare them against practices observed in a recent audit of a telecommunications company conducted by the ODPC.

AGS outlined that it had established a single contact point for such requests in 2008 which it referred to as its Telecommunications Liaison Unit. AGS confirmed that requests made under the Communications (Retention of Data Act) 2011 are made by AGS via this limited set of designated points of contact (15 individuals) based in the Telecommunications Liaison Unit, Crime and Security, Garda HQ, Phoenix Park.

AGS outlined to the Team its criteria when making a request for communications data

a) was AGS legally covered
b) could AGS demonstrate relevance
c) could AGS demonstrate necessity
d) is the data being sought proportionate e.g. not all traffic data at 3am in Lucan – narrow the request down further

AGS outlined to the Team the Communications (Retention of Data) Act 2011 reduced the length of time required of telcos to retain call traffic data from three years to two and introduced a one year retention period for internet traffic data.

AGS referred to the oversight procedures in place based on the legislation, namely the annual review and examination of requests by a Judge to ensure all data sought by AGS was sought legitimately within the confines of the legislation.

With regard to criminal justice terrorist offences and call related data, AGS clarified that since the Communications (Retention of Data) Act 2011 came into force, AGS would also seek subscriber information as provided for under the provisions of schedule 2 of the Communications (Retention of Data) Act 2011)[24].

[24] Under previous legislation (e.g. the Criminal Justice (Terrorist Offences) Act 2005) such requests would not have allowed for the seeking of subscriber information and so AGS would have sought to invoke section 8 (b) of the Data Protection Acts instead.

In terms of the provision for disclosure in Section 8(b)[25] of the Data Protection Acts, the ODPC pointed out that this provision is permissive only and it does not place any obligations on data controllers to provide An Garda Síochána with personal data. This provision carries the qualifier "in any case in which the application of (data protection) restrictions would be likely to prejudice (preventing, detecting or investigating offences)." Therefore, the exemption does not cover the disclosure of all personal information held by a data controller, in all circumstances.

Overall, the ODPC considers that the key difference between the Communications (Retention of Data) Act 2011 and section 8(b) of the Data Protection Acts is that the former provides for mandatory disclosure where serious offences are concerned. The latter allows for voluntary disclosure subject to consideration on a case-by-case basis as to whether not releasing the data would be likely to prejudice (that is, significantly harm) any attempt by organisations which have crime prevention or law enforcement functions to prevent crime or to catch a suspect. AGS confirmed that it would seek to rely on section 8 (b) of the DP Acts for all data sought in relation to non-serious crime requests.

With regard to PIN and PUK information (credit and top-up details), AGS indicated that if this data was required it would seek to rely upon section 8 of the Data Protection Acts as this type of data was not explicitly referred to in the 2011 Act.

On the day of the inspection AGS stated that a telecommunications company had asked AGS to cite both acts when making requests. We indicated to AGS that we do not consider this approach to be valid and are of the view that all data sought by AGS under section 8 of the Data Protection Acts should rely on that Act only and equally the same would apply for requests made under the Communications Retention of Data Act 2011. During the course of its audit that same telecommunications company, it was suggested by the ODPC that any request for data relating to a serious offence should be made entirely under the 2011 Act and requests for all data in relation to non-serious offences could be handled under section 8(b) of the Data Protection Acts. The telecommunications company indicated this would be a practical and workable change. AGS confirmed that this is already the case i.e. the Communications Retention of Data Act 2011 is used for requests for data for serious offences, and the Data Protection Acts are used where the 2011 Communications Retention of Data Act would not apply i.e. non-serious offences. AGS indicated that section 8 (b) of the Acts would also be used if AGS sought data such as credit top up information, purchase details etc which were not specified in the 2011 Communications Retention of Data Act.

The ODPC also notes all requests made under the Communications (Retention of Data Act) 2011 place a mandatory requirement on data controllers to provide the data whereas requests made under the Data Protection Acts are to be considered on a case-by-case basis by the data controller.

We signalled to AGS our intention to engage with AGS further on this in order to develop and issue sectoral advice to all telcos in this regard.

[25] "Any restrictions in this act on the processing of personal data do not apply if the processing is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid"

The Team referred to an audit it conducted of a technology company and how during the course of an inspection it had viewed a request from AGS to that company which cited the 2011 Communications (Retention of Data) Act as the legal basis to seek the data. The Team explained to AGS that the ODPC had advised the company that it was not covered under the 2011 Communications (Retention of Data) Act.

In terms of oversight within AGS, the Team asked AGS to demonstrate how it ensured that a request was a valid request for disclosure within the terms of the legislation cited. AGS outlined to the Team that 10% of all requests are reviewed as part of an internal audit held every three months. AGS outlined that when a request is created a unique reference number for that request is generated and a pdf created to ensure the wording of the request cannot be altered. AGS clarified that, if a request is cancelled, it would still be stored on the system but, for example, in the internal audit would come up marked in yellow to signify it was cancelled. AGS also stated that the audit would also compare the unique reference numbers of requests cancelled. The Team viewed a number of requests for disclosure and AGS provided examples of requests refused internally (e.g. request no. 201/7/11).

AGS referred to a number of HQ Directives providing guidance on this area and the Team requested specific references for these Directives in case of future oversight requirements. AGS in response stated that HQ Directives 24, 25, 26, 27 & 28 of 2013 provide instructions and guidance in relation to requests for communications data.

AGS stated that in total 1,829 requests for disclosure were made to telcos in January 2012 and these figures when broken down consist of: 1,296 subscriber requests; 494 call trace requests; and 39 ip requests. AGS clarified that these inquiries were made under either the Communications Retention of Data Act 2011 or the Data Protection Acts 1988 & 2003.

The Team proceeded to cross-check and examine a range of disclosure requests made by AGS to a telecommunications company to establish whether the Team considered the sample set of requests made by AGS were valid having regard to the legislation concerned. [*These samples were collected as part of an audit conducted by the ODPC of this company in February of 2012.]*

Requests made in line with the provisions of Section 6(1) of the Communications (Retention of Data) Act 2011.

1. **18 January 2012:** The first sample was a list sent to the company of 36 phone numbers by AGS Crime & Security seeking subscriber data. The list was a follow-up to these details having been requested by phone. The Team noted that the request sent was signed by the Chief Superintendent but this was after the telephone request had already been made by a staff member in Crime & Security. The rationale given by AGS for this was that the volumes of requests for subscriber data make it virtually impossible for all such requests to be signed in advance by the Chief Superintendent and that as these requests may be in the order of circa 40 a day this was seen by AGS as a practical solution.

   The ODPC selected two phone numbers at random from this list and examined the background to the cases. The first involved the theft via an ATM of 2 x 100euro where the PIN code had been obtained on a fraudulent basis. AGS stated this fell under the legislation deeming it as a serious offence as it was an indictable crime with a possible sentence of more than 5 years. The second of these involved a fraudulent bank draft being produced as payment for four alloy wheels-value circa 1000 euro.

2. February 2012: A Murder Crime, all appeared in order with incoming and outgoing calls sought.

3. July 2011: Three official AGS phones stolen from a locker in a gym. Call traffic data requested. This Office did have some reservations as to whether this was an appropriate use of the legislation. AGS stated that theft is an indictable offence.

4. July 2011: Investigation of a robbery/sexual assault. All data retained in line with Section 3 and provided for in part 1 of schedule 2.

5. Requests made for subscriber details in line with the provisions of Section 8 (b) of the Data Protection Acts 1988 & 2003.

July 2011: Attempted intimidation of a Garda by calling them on their phone. AGS sought purchase details and top-up data.

6. Requests made for subscriber details in line with the provisions of Section 8(d) of the Data Protection Acts 1988 & 2003.

November 2010- a woman phoned a Garda station to report a firearms discharge but did not leave her contact details. AGS stated it needed to follow up with her to prevent any threat to injury and as a witness so the purchase details of the phone were sought.

Overall, the Team were satisfied with the procedures in place and the system for internal review. However the situation where a request is made without the Chief Superintendent's knowledge and signed/authorised retrospectively by the Chief Superintendent was not considered by the Office to follow the requirements specified in the Communications (Retention of Data) Act 2011. The Team advised AGS that all requests for call and internet traffic data should be authorised by the Chief Superintendent on a case by case basis rather than on an aggregate basis at the end of a particular time period.

AGS responded indicating that this process referred to subscriber requests only. AGS confirmed that a change of process has been implemented and all applications are now approved by the Chief Superintendent in advance. AGS further clarified that each application is considered separately on a case by case basis on its own merits. AGS confirmed that the Chief Superintendent only reviews the list in those instances but all the information would be reviewed in the internal audits of all requests made which AGS stated is carried out on a 3 monthly basis.

The ODPC also notes that the Communications (Retention of Data Act) 2011 refers to data as meaning

> "traffic data or location data and the related data necessary to identify the subscriber or user".

Schedule 2 of the Act further outlines

PART 1
Fixed network telephony and mobile telephony data to be retained under section 3

1. Data necessary to trace and identify the source of a communication:
(a) the calling telephone number;
(b) the name and address of the subscriber or registered user.

2. Data necessary to identify the destination of a communication:
(a) the number dialled (the telephone number called) and, in
cases involving supplementary services such as call forwarding
or call transfer, the number or numbers to which
the call is routed;

(b) the name and address of the subscriber or registered user.

The ODPC considers that the Communications (Retention of Data Act) 2011 allows for the provision of both Call Data Records (CRD) (traffic data or location data) and subscriber data (the data necessary to identify the subscriber or user). Call Data Records include details of the number calling and the number called, type of call – voice, SMS etc, details of handset used, start/finish time of call and where call entered system, i.e. mast.

One outstanding area of attention requiring the advice of the ODPC following the audit of a telecommunications company is the period for which all records requested by AGS/Revenue/Defence Forces should be retained thereafter by the telecommunications companies.

Section 4 (d) of the Communications (Retention of Data) Act 2011 states

> "the data, **except those that have been accessed and preserved**, shall be destroyed by the service provider after[26]"…

The ODPC asked AGS if it had considered the retention aspect of procedures under the Act and whether it would signal to a telecommunications company upon release of the data to AGS whether the company also needed to retain a copy for a certain period also and if so how long for.

AGS indicated in response that the advice of the Attorney General has been sought in this regard and that its current policy was that a "golden copy" (copy of the data already supplied) is to be retained by the Communications Service Provider (CSP), with the period of retention not yet agreed. AGS stated that all CSP's will be informed of an agreed time frame. The ODPC intends to actively engage with AGS further on this issue in order to develop and issue sectoral advice in this regard.

During the inspection, the telecommunications company indicated that when processing a data subject access request made under section 4 of the Data Protection Acts, it would not provide to the requesting data subject any information relating to requests that may have been made to it by An Garda Síochána under the Communications (Retention of Data Act) 2011.

The Inspection Team advised the company that requests for disclosure from AGS, Revenue or the Defence forces should be considered for release as part of a section 4 access request and should only be withheld if AGS/Revenue/Defence Forces confirm that release would prejudice the investigation, prevention or detection of a crime – i.e. that the restriction on the right of access under section 5(1)(a) applied.

The company responded stating that the current protocol in operation is that any section 4 access requests which could potentially entail disclosing to a data subject request for information details of AGS/Revenue/Army requests would be referred back to the relevant agency unless they were informed that the investigation or national security incident relating to the request had concluded. The ODPC advised the company that it considers it to be a data controller at all times in this context. In relation to this issue, the retention period for which the company would hold a copy of such access requests in the first place is highly relevant and so the seeking of advice by AGS from the Attorney General in this regard was noted.

[26] 2 years and one month and one year and one month

Again AGS indicated that this issue will be discussed with the service providers and agreement will be reached on how to address the issue going forward. The ODPC intends to actively engage with AGS further on this issue in order to develop and issue sectoral advice in this regard.

9. Arrest and Detention

The processing of personal data in the context of the arrest and detention of an individual was examined in detail in the context of an on-site inspection at Mullingar Garda Station. It was also examined during an on-site inspection at Donnybrook Garda station.

The Team commenced the inspection by examining the flow of personal data from the time a person is arrested and detained in custody until they are released and/or charged and subsequently referred to the Courts. A key focus of the audit was to examine the procedures for recording data entered onto PULSE as well as physical security procedures and practices within Mullingar Garda Station.

AGS Mullingar outlined the various grounds under which a person might be arrested or detained, explaining that typically a person might be arrested for the purpose of charge under section 4 of the Criminal Justice Act 1984 or section 2 of the Criminal Justice (Drug Trafficking) Act 1996. However, a person might only be detained by AGS (as opposed to arrested) for the purposes of a search under section 23 of the Misuse of Drugs Act. AGS Mullingar outlined that in a large number of cases a person might be arrested for public safety reasons where a disruption to public order has occurred. In this context, AGS referred to sections 4 and 5 of the Criminal Justice Public Order Act 1994 relating to intoxication in a public place/disorderly conduct and section 15 of the same Act which relates to violent disorder.

AGS Mullingar stated that all individuals arrested/detained would be informed of their rights and provided with a copy of **Form C72 -'Information for Persons in Custody'** -Regulation 8 of the Criminal Justice Act 1984 (Treatment of Persons in Custody in Garda Síochána Stations) Regulations 1987 and 2006..

AGS Mullingar indicated that all individuals arrested/detained are first taken to the custody area and interviewed by the Sergeant on duty. A **Custody Record** which captures the details of the person in custody and the circumstances of their arrest/detention is completed by the 'Member In-Charge' or a member of An Garda Síochána authorised to do so by that 'Member In-Charge' in accordance with the Criminal Justice Act, 1984 (Treatment of Persons In Custody) Regulations 1987.

In terms of establishing or verifying the identity of a person, AGS stated the individual may have identification documentation on their person which AGS will use to run a check on PULSE or the person may give an address which AGS can check by sending a Garda car to verify the address is the principal residence of the individual in custody as confirmed by other householders or neighbours. AGS outlined the importance of verifying identity in terms of any pending prosecutions.

The Team noted the emphasis placed on verifying identity in a document provided to the Team entitled **'Adult Caution – Decision to Prosecute.'** Here, it is stated,

> Identity of offender; The Garda must be 100% certain as to the identity of the offender before initiating a prosecution. Checks must be made with the prisoner and also at the address given. Photographs should be taken either with consent or in accordance with Section 12 of the Criminal Justice Act.

> Gardaí should not accept a name, address or date of birth as genuine just because it matches an existing record on Pulse. Further checks must be made, there may be a photo on Pulse, he may be known to other Gardaí, ask who his neighbours are, names of his mother and father, check for scars, tattoos.
>
> When recording a person on Pulse ensure all scars and tattoos are recorded in their description details on Pulse.

The Team confirmed with Mullingar AGS that every individual arrested or detained will have their details entered onto the Custody Record.

Once the Custody Record is completed, AGS Mullingar stated that all individuals in custody are placed in a holding cell and taken to the interview room if an interview is necessary. AGS confirmed to the Team that not all prisoners are interviewed and the decision to interview a prisoner will depend on the circumstances of the arrest and legislative provisions (e.g. a drunk driver would not normally be interviewed).

The Team visited the interview room and observed the monitor and camera where the recording of interviews –audio and visual- takes place. The Team noted the camera is focused on the individual being questioned who sits in a chair which is fixed to the ground so that the area being recorded is consistent. The Team examined the CCTV in place in the interview room and noted that the interviewing officers are visible in the footage also (in the top left hand corner of the screen). The Team also visited the storage area where the CCTV tapes are stored and AGS indicated that a copy of the interview tapes can be requested by the defence on foot of a court order issued by a judge. AGS stated that there are 3 copies of the footage recorded with the master copy set aside for the court.

The ODPC advises AGS that an individual may also request a copy of CCTV interview tapes containing their personal data under section 4 of the Data Protection Acts in certain instances. However AGS would be entitled to consider refusal of the tapes if a prosecution was pending or if AGS could demonstrate the supply of the data could prejudice an investigation. Section 5 of the Data Protection Acts provide that individuals do not have a right to see information relating to them if the data is being

> 5. 1 (a) kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of that section to the data would be likely to prejudice any of the matters aforesaid

Mullingar AGS demonstrated to the Team that each Custody Record Book contains 10 custody record sheets in total and once all ten records have been completed the custody records are sent for storage. The Team viewed the office where custody records are stored which AGS Mullingar stated is locked when unoccupied. When occupied, AGS stated that only the Sergeant on duty can issue custody records to members who must sign-out any custody records obtained and sign-in again to verify their return.

9.1 Prisoner's Log

AGS Mullingar outlined that all prisoners are also recorded onto a **Prisoner's Log** – even if the individual arrested is subsequently released without charge. The Team

enquired as to the difference between the Prisoner's Log and the custody record. AGS clarified that a 'Prisoner Log' is a PULSE record that is created for every person who is brought in custody to a Garda Station. This record is created from a PULSE incident and is linked to a Person record. The 'Prisoner Log' contains basic information in relation to the arrest.

In contrast, AGS outlined that a Custody Record Form C (84) contains a detailed manual record that is completed for every person who is brought in custody to a Garda Station as required by the Criminal Justice Act, 1984 (Treatment of Persons In Custody) Regulations 1987. The Custody Record is used to record an in-depth contemporaneous account of the details, actions and occurrences relating to the prisoner during their time in custody. Each entry in the Custody Record is signed or initialled by the member making it.

9.2 Potential Outcomes of Arrest/Detention

In terms of potential outcomes, AGS stated that a decision will be made by AGS to charge the individual, release the individual without charge, or to issue them with a written caution.

9.3 Charge Sheet

AGS clarified to the Team that only individuals who are actually charged and either detained or released on bail will be entered on the charge sheet. If an individual is released with a summons, there is no charge issued to them on the night and their details will not be entered on the charge sheet. AGS clarified that all summons are signed by the relevant District Court.

AGS also stated that every individual charged will get a copy of the charge sheet and the court will receive the original charge sheet with the Garda member retaining a copy also.

9.4 Decision to Prosecute

If an individual is charged they may be released on bail or alternatively they may be held in custody until they appear before a sitting of Mullingar District Court.

AGS Mullingar referred to the necessity to appoint a dedicated officer who is responsible for all documents going to the courts, noting the court list and arranging to obtain copies of court orders referred to as 'Gary Doyle orders' which is an order giving the details of all evidence against the person being prosecuted.

AGS stated that under section 8 of the Garda Síochána Act, AGS have the authority at District Court level for an Inspector or Superintendent to present in Court as the prosecutor and utilise the advice of the State Solicitor if required. In the District Court, AGS reiterated that the Courts Service record all the district court outcomes and these are electronically fed into PULSE via the CJIP service (data feeds between Courts Service and AGS). AGS stated that a certified copy of the court outcome would only be sought by AGS if the outcome was challenged.

At Circuit Court level, AGS confirmed that the State Solicitor would prosecute with the assistance of the Director of Public Prosecutions (DPP) if required. In terms of

Circuit Court outcomes, AGS stated that the Sergeant present in Court has responsibility for recording the outcomes accurately onto PULSE.

The Team considered that based on the information supplied by AGS there were no data protection issues arising with regard to the processing of data in connection with arrest and detention procedures.

10. Disclosure of Personal Data to Third Parties

The Audit Team's examination of disclosure of personal data between AGS and the HSE (for child protection), the Department of Transport (for road traffic), the Courts Service and the Prisons Service has been described above in sections 4 and 5. The issue of disclosures of personal data at the level of individual Garda stations was a focus of an on-site inspection at Donnybrook Garda Station.

10.1 Road Traffic Accident.

The first request for disclosure viewed by the Team was a letter from a solicitor acting for a named client on foot of a road traffic accident seeking the

1. Details of Investigating Garda.
2. Name and address of all parties in the said accident.
3. Registration Details of all vehicles.
4. Details of all Insurance cover and Policy numbers.
5. Name and addresses of any independent witnesses.
6. Whether a Prosecution under the Road Traffic Acts is contemplated.
7. Any copies of any statements and any sketch if available.

Regarding requests seeking driver details based on the provision of a vehicle registration number, the ODPC is aware that under the Road Traffic Acts 1961, section 106, an injured party or someone representing the person such as a solicitor is entitled to get basic driver information from An Garda Síochána.

The Garda Síochána Data Protection Code of Practice cites this facility as one example of a legitimate disclosure as

> "a member of An Garda Síochána providing the registered owner details of a car to an injured party under the provisions of the Road Traffic Act or to a person legitimately representing their interests." (p.12)

The Team noted the solicitor seeking the data did not cite any provisions of the Road Traffic Act in its request, except to enquire as to whether a prosecution under the Road Traffic Acts was contemplated. AGS outlined to the Team that it would supply information relative to the solicitor's request in line with the provisions of the relevant Road Traffic Acts and that a request should not be rejected where the solicitor is entitled to the information on behalf of their client, solely based on an omission on citing the relevant provisions of the Road Traffic Acts. As best practice we consider that AGS should encourage solicitors making these requests to cite the relevant provisions of the Road Traffic Acts in this regard.

The Team enquired as to exactly what data would be disclosed back to the solicitor on foot of such a request. AGS Donnybrook referred the Team to AGS Form A.65

which the Team determined was an abstract of a traffic accident report. The Team reviewed the 11 categories of data supplied on the abstract sheet and deemed them to be comprehensive including copies of statements and a sketch if requested (and if the sketch had already been prepared). In terms of the request for details of insurance cover and policy numbers, the Team noted the abstract only provided the name of the insurance company in relation to each of the vehicles involved.

In terms of the extent of data disclosed by AGS in these instances AGS informed the Team the Garda Code Chapter 24(5) provides the current and most up to date instructions regarding Road Collision Abstracts as follows:

(a) Persons involved in road collisions, their legal advisers or insurers or other interested parties may, on written request, be supplied with an abstract of police report, copies of statement of witnesses and sketches or maps of the scene.

(b) The abstract will not be supplied if criminal proceedings are contemplated or initiated.

(c) The abstract will be furnished on Form A65 without giving any additional information. It is strictly forbidden to include suspicions, inferences, opinions or hearsay in Garda statements or abstracts.

(d) In the case of fatal road traffic collisions, the abstract will not be supplied until the inquest concerning the death has been completed by the Coroner.

(e) Where the collision results in material damage only, members should not make enquiries for the sole purpose of preparing abstracts. This is not to be construed as a reason for overlooking other offences, which may be disclosed or detected at the scene.

(f) When abstracts of police reports on road traffic collisions are being supplied, the policy number or other company reference regarding the injuries of other parties to the collisions should be furnished. Members to whom Insurance Certificates are produced should note carefully and record the policy number or other company reference.

(g) Abstracts of police reports of road collisions, sketches or maps and copies of statements will be furnished by the District Officer of the area where the collision occurred. Where for any particular reason, abstracts of police reports cannot be furnished on demand, the names and addresses of vehicle owners and witnesses to collisions may be supplied free of charge, on request, to parties to such collisions and their legal advisers.

(h) Fees at current rates are charged for abstract copies of witness statements and photographs in the case of road collisions supplied to members of the public. A fee, at current rates, will also be charged to recoup Garda costs involved in the supply of photographs to interested parties in case of collisions involving death or serious injury. When forwarding such documents, the District Officer should clearly request that the cheque be made payable to the Superintendent of the area where the collision occurred.

(i) Where for any particular reason, abstracts of police reports cannot be furnished on demand, the names and addresses of the vehicle owners and witnesses to collisions may be supplied free of charge on request to parties to such collisions or their legal advisers.

AGS Donnybrook also provided the Team with a copy of a Garda Síochána Road Traffic Accident Report CT'68. The report contained extensive detail as to the accident including vehicle, driver and passenger details as well as a section entitled ‘contributory factors’ which in terms of a single principal causing the accident described driver 2 ‘to a large extent and driver no 1. ‘not at all’ . AGS confirmed to the Team that only an abstract relating to the Traffic Collision (Form A65) can be

requested subject to receipt of the appropriate fee. The Road Traffic Collision Report (CT'68) is not disclosed.

The Team enquired whether after a period of time elapsed i.e. a case involving a road traffic accident had gone to court and a verdict reached, AGS would supply the Road Traffic Collision Report (CT'68) as part of an access request made under section 4 of the Data Protection Acts by one of the individual's involved. AGS responded that when court proceedings have been instigated, it is normal practice to provide an Abstract Report of the traffic collision with accompanying statements on receipt of the appropriate fee. AGS confirmed that it is not Garda policy to provide PULSE generated reports of traffic collisions as part of Section 4 access requests.

On the day of the inspection AGS Donnybrook also referred to summaries of the road traffic accident reports being issued to the Road Safety Authority for statistical analysis. The Team noted the details sent to the RSA did not contain the names of the parties involved but did contain the vehicle registration details which the Team considered based on data available to the RSA on other databases would render the persons identifiable.

AGS clarified that in fact the complete CT'68s (Road Traffic Collision Reports) are currently forwarded to the Road Safety Authority (RSA) via post - the CT'68s in the case of fatal collisions are forwarded from District offices to Garda National Traffic Bureau (GNTB) who then forward them via post to the RSA. Forms for other collision types continue to be forwarded directly from District offices to RSA.

AGS outlined that the CT68's have been provided since 1968 and that originally they were provided by District Offices to the National Roads Authority (NRA).

The Road Safety Authority Act 2006 established the RSA and Section 8(3) outlined hereunder provides for provisions of statistics (i.e. via form CT68)

> 8.(1) The Minister may direct the Authority to collect, compile, prepare, publish or distribute to such persons (including the Minister) such information and statistics relating to road safety and the functions of the Authority, as the Minister considers appropriate, for national or international planning, policy research and development, monitoring and reporting purposes and may specify any matter concerning the collection, compilation, preparation, publication and distribution of such data and statistics, as the Minister considers appropriate.
>
> (2) The Minister shall consult the Authority, and may consult any other person he or she considers appropriate, before issuing a direction under subsection (1).
>
> (3) For the purpose of facilitating the collection of information and statistics under subsection (1) the Authority may require a person who holds records relating to road safety or matters relating to the functions of the Authority, to give to the Authority such information and statistics in such form (including electronic form) and at such reasonable times or intervals, as the Authority specifies. A person to whom such a requirement is directed shall comply with the requirement.

10.2 Insurance Company

The second request for disclosure viewed by the Team was a letter from an insurance company (Allianz) seeking further details on a claim in relation to stolen property.

A tick box set of questions was provided for AGS to tick

- Was this incident reported to you?
- Has anyone been made amenable for the crime?
- Had any of the stolen property been recovered?
- Have there been previous incidents of a similar nature for the above mentioned person
- Stolen property includes: laptop, cash

With regard to the question asked by Allianz **'Have there been previous incidents of a similar nature for the above mentioned person'** the ODPC does not consider there is a basis under the Data Protection Acts for AGS to provide this information to Allianz. The insurance sector already has access to a sectoral insurance claims database - **Insurance Link**- and thus it can search this database in relation to any previous claims made by individuals in relation to stolen property, house insurance, personal injury etc. This Office does not consider insurance companies should be made privy to previous incidents of stolen property reported to AGS, for example a mobile phone.

In this context, the Team discussed a specific case with AGS Donnybrook pertaining to a reported break-in to a woman's car the day before. The woman was claiming to AGS that property worth 12,000 euro including gold and diamond jewellery and designer sunglasses had been stolen from her car and that she had left the items in her car overnight. AGS noted there was no sign of forced entry and the woman stated that she had locked the car with her fob key and so could not understand how they broke into the car. AGS offered to do a forensic search of car for fingerprints but the woman declined saying she planned to sell the car later that day.

The Team viewed the standard tick box set of questions in relation to a claim of theft received from one insurer and enquired whether AGS would provide additional relevant information to the insurers and AGS indicated that if they suspected fraud they would do so.

The Team considered that based on the information supplied by AGS there were no data protection issues arising with regard to the processing of data in relation to disclosures to and from 3rd parties.

11. Use of CCTV Systems

AGS make extensive use of CCTV for crime investigation and prevention purposes. Some CCTV systems are under direct AGS control. Others are operated by community groups with the approval of AGS. AGS also seek copies of relevant CCTV footage from other data controllers when investigating crime. These different uses of CCTV by AGS were examined in the context of an on-site inspection at Limerick Garda Station[27].

11.1 Garda CCTV Scheme

The focus of the Limerick inspection was to assess the use of a Garda controlled CCTV scheme. The legal basis for the use of CCTV by AGS is set out in Section 38 of the Garda Síochána Act 2005. In addition, the operation of CCTV is governed by

[27] The Garda CCTV system in operation in Mullingar was also inspected as part of the inspection of Mullingar Garda Station

the **AGS Policy for Closed Circuit Television in Public Places** and the **AGS Code of Practice for Closed Circuit Television in Public Places**. AGS stated that these two documents were issued as part of a HQ Directive 82/09 issued on 09 June 2009.

The AGS Code of Practice for Closed Circuit Television in Public places responsibility for oversight for standards of existing systems and new applications with the CCTV Advisory Committee, chaired by the Chief Superintendent Community Relations. The overall management of a CCTV scheme and the requirement to comply with the code of practice is the responsibility of the local Divisional officer.

The CCTV system concerned is located in the Divisional Communications Room, to which access is restricted by a key pad entry system. Along with monitors connected to it's own 32 cameras, the Team was informed that AGS has access to 2/3 community CCTV Systems comprising over 100 cameras, as well as 18 traffic cameras operated by the local authority. AGS stated that it only has viewing access to these external CCTV systems; it cannot manipulate or download footage from them. However, AGS stated that if it requires footage from these systems, it requests the footage from the data controller concerned. The station's internal CCTV system is also viewable on the same monitors.

AGS outlined that the CCTV system cameras and video links, CCTV monitors and CCTV control are maintained by company X. The DVR was supplied by company Y. Company Y will repair the DVR if it becomes faulty. AGS confirmed to the ODPC that neither company X or company Y have access to any recorded material as they do not have user accounts on the system. The system is administered by Garda Telecommunication staff based in GHQ.

11.2 Operator Responsibilities for Garda Town Centre CCTV Systems.

Section 4 of the **AGS Code of Practice for Closed Circuit Television in Public Places** sets out an operator's responsibilities. These include:

> 4.1(i) "All staff performing duty in the CCTV monitoring area will enter in the CCTV Incident Log Book details of the time and date of commencement and completion of such duty."

There was no evidence available to the Team that this was the practice in Henry St. Garda Station. The Team recommended that in line with Section 4.1(i) all staff performing duty in the CCTV monitoring area should enter in the CCTV Incident Log Book details of the time and date of commencement and completion of such duty.

[Since the inspection took place, AGS stated that it is now operating in compliance with section 4.1(i) of the Code of Practice for CCTV in Public Places in relation to staff performing duty in CCTV monitoring areas.]

AGS clarified to the Team that the CCTV monitoring area for Limerick City is incorporated into the Divisional Communications room at Henry Street and is monitored by staff deployed there. All staff are attached to the rostered working unit and sign on, in accordance with code instructions, in the station diary. Entries in the station diary and on forms D.27 provide for an effective audit trail identifying pertinent staff.

Since the inspection took place AGS informed the Team that in order to ensure precise compliance with policy in this area a sign-on book has been introduced and is in operation since February 2013. The ODPC welcomes the introduction of this practice.

Section 4.1(ii) of the **AGS Code of Practice for Closed Circuit Television in Public Places** states that

> "Cameras will not be used to look into any premises, be they public houses, shops, business or private dwellings. Likewise this form of invasion of privacy applies to any demonstration of the capabilities of the cameras. Cameras can be shown to be efficient without looking into premises".

The Team was informed that this provision is strictly adhered to and under no circumstance would the zoom function of an AGS CCTV camera be used to view into a business premises or private residence.

11.3 CCTV Review Facility

Section 5.2 of the AGS Code of Practice for Closed Circuit Television in Public Places) states:

> "The review facility at each respective location will only be used by Garda members authorised by the local District Officer to make use of that facility for the purpose of reviewing a videotape recorded on that or another similar system. Any member making use of the review facility must complete an entry in official documentation, which will also include the Superintendent's authority."

The Team examined the operation of the CCTV review facility in operation at Henry St. Garda Station. The Team was informed that the normal process is that a request, by email, is made to the Sergeant in charge, who forwards it on to the reviewer. AGS clarified to the Team that two people in Limerick AGS are authorised to review & download CCTV footage, one a Garda member and a civilian staff member.

In relation to reviews only where information is not downloaded, AGS indicated that a generic username and password would be used by Garda members to view recorded material on the CCTV system. AGS stated that the requirement of the CCTV Code of Practice that each review should include the Superintendent's authority is impractical, given the volume of reviews being undertaken. AGS indicated that these comments are noted by the CCTV Review Group and cognisance is being taken of this issue as part of the CCTV review.

Access to download footage from the CCTV system is restricted to two individuals who have a specific username and password. The Team was informed that the CCTV footage is downloaded either in the server room, which is off the Communications Room and normally locked or in the Station's IT room.

AGS stated that no record is retained by the system where CCTV footage is reviewed; however, a manual log or register is maintained if CCTV footage is downloaded. The Team was shown the log of CCTV downloaded which is kept in a hard-backed journal. The Team examined this log and noted that the date, location

and duration of footage are recorded along with the name of the Garda member making the request. However, the Team noted that there was no justification for accessing the footage or any PULSE number recorded against the download record. OPDC recommends that a PULSE incident number be recorded in respect of each download from Garda CCTV footage accompanied by a brief justification.

The Team also questioned if an audit trail was available for footage downloaded from the Garda CCTV system and was informed that there is no audit trail. AGS subsequently confirmed that the CCTV system installed in Henry Street Station does not include functionality that would allow an audit log of the reviewed or downloaded material to be recorded. In that case, the Team indicated that a manual audit trail/record of CCTV material that has been reviewed or downloaded is required to be maintained.

In response, AGS stated that the need for absolute accountability in relation to the review of CCTV footage has been recognised by the CCTV Review group and cognisance has been taken of this in preparing the updated Code of Practice. In the meantime, AGS referred to the current Code of Practice which outlines the following instructions in relation to the review of material:

> *Code of Practice 6.2*: The review facility at each respective location shall be accessed only by Garda members authorised by the local District Officer to make use of that facility for the purpose of reviewing video material recorded on that or another similar system. Any member making use of the review facility must complete an entry in official documentation, which will also include the Superintendent's authority.

The Team examined five entries in the CCTV log and using the date and location, AGS were able to identify incidents on PULSE which related to the downloads requested. However, in relation to one incident, concerning a request from a Garda Sergeant to have three hours footage downloaded from the camera in the public office area of Henry St. Garda Station, no specific justification was provided. AGS subsequently reverted that this download did not actually take place and that the footage was only viewed to identify a theft of Garda property on the data in question. AGS stated that

> "It appears that a station stamp went missing from the public office and was suspected to be stolen. It subsequently was located in the station later. However at the time it went missing there was a suspicion that a caller to the station could have taken it and the request was made to access the video footage. No incident was created as it was subsequently discovered not to have been stolen."

A member of Telecoms staff was present on the day and the log maintained did not specify details of the request. In all other cases, the PULSE ID was recorded. AGS confirmed that there was no PULSE incident created for the query concerning the missing Garda Station stamp.

11.4 Use of 3rd Party CCTV Footage

The Team noted that it is also the practice of Garda stations to download footage which may be required for an investigation from the CCTV systems of other data controllers.

Section 8(b) of the Data Protection Acts 1988 and 2003 states, inter alia, that any restrictions in this Act on the processing of personal data do not apply if the processing is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid.

The ODPC pointed out to AGS that provision for disclosure in Section 8(b) is permissive only and it does not place any obligations on data controllers to provide An Garda Síochána with personal information from their CCTV systems. This provision also carries the qualifier "in any case in which the application of (data protection) restrictions would be likely to prejudice (preventing, detecting or investigating offences)." Therefore, the exemption does not cover the disclosure of all personal information held by a data controller, in all circumstances. It only allows for the disclosure of personal information for the stated purposes if not releasing it would be likely to prejudice (that is, significantly harm) any attempt by organisations which have crime prevention or law enforcement functions to prevent crime or to catch a suspect.

The Team was informed that the procedure in Limerick AGS for collecting CCTV from third parties is that a reviewer calls to the premises concerned, views/downloads the CCTV requested by the investigating Garda and in exceptional circumstances, the CCTV system may be removed from the premises by an Garda Síochána. All such downloads are recorded in the AGS manual log. AGS informed the Team that it does not make such requests in writing and that, given the volumes of external downloads, which may be up to six in a day, this would be impractical. However, the Team was informed that business owners are very cooperative in this area. AGS informed the Team that the legislation covering the awarding of Special Exemption Orders used by Nightclubs, the Intoxicating Liquor Bill 2008, has a specific requirement for adequate CCTV on the premises.

The Office considers that, given that CCTV is obtained using a specific permissive clause of the Acts, requests for downloads of CCTV footage made by AGS to third parties should be followed up in writing at all times. Any such requests should be on Garda headed paper, quote the details of the CCTV footage required and should also cite the legal basis for the request i.e. Section 8(b) of the Acts. ODPC does not consider that it would be operationally difficult for AGS to introduce a template for such requests.

AGS responded indicating that all matters pertaining to Garda CCTV are being reviewed at this time. A large body of case law has addressed issues in relation to the need for statements of evidence to be taken from third parties in obtaining evidence (e.g. Braddish v DPP, Dunne v DPP). Dunne v DPP (2002) Supreme Court- It is the duty of the gardaí, arising from their unique investigative role, to seek out and preserve all evidence having a bearing or potential bearing on the issue of guilt or innocence (Hardiman J).

11.5 Retention and Storage.

The Team was informed that Garda CCTV footage is retained for 31 days, except where it has been selected to be downloaded and retained. AGS stated that in such cases the CCTV footage is stored on either a USB key or disc in the incident room under the responsibility of the exhibits officer and will only be released for official

AGS purposes or to the defence team in a case for prosecution, under the judicial discovery process.

11.6 Access to Garda CCTV by third parties.

Section 38(1) of the Garda Act 2005 states that

> "the Garda Commissioner may authorise the installation and operation of CCTV for the sole or primary purpose of securing public order and safety in public places by facilitating the deterrence, prevention, detection and prosecution of offences."

In addition Section 8.1of the **AGS Code of Practice for Closed Circuit Television in Public Places** states that "video recordings will be used for Garda purposes only and on no account will they be released to outside bodies or individuals for private or civil use except where such has been ordered through the normal judicial process. Any cases of doubt will be referred by the local district Office to Assistant Commissioner, Crime and Security for instruction. "

AGS informed the Team that this provision is strictly complied with and CCTV footage is only released to third parties through the discovery process. The Team enquired if there were any circumstances whereby CCTV footage would be released on foot of an access request under Section 4 of the Acts. AGS stated that that it could not envisage any circumstances whereby an excerpt of CCTV footage recorded by it would be released to a third party. In addition, AGS stated that it has not received any request from their local authority, for instance, for CCTV to be used in any prosecution under the Litter Pollution Acts, as amended by the Waste Management (Amendment Act) 2003.

The position of the ODPC is that there are some very limited exemptions to a data subject's right of access which are set out in Sections 4 and 5 of the Acts. Section 5 of the Acts provides that individuals do not have a right to see information relating to them where certain circumstances apply including where the information is kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing/collecting any taxes or duties: but only in cases where allowing the right of access would be likely to impede any such activities. ODPC considers it would be unacceptable to allow a criminal suspect to see all of the information kept about him by An Garda Síochána, where this would be likely to impede the effectiveness of the criminal investigation. On the other hand, however, if allowing an individual access to personal information about him or her would not be likely to impede an investigation, then the access request would have to be complied with. In addition, it may be the case that such information should be considered for release when an investigation has been concluded.

It is therefore recommended that AGS should review its policy for handling requests for access to AGS CCTV footage made under Section 4 of the Acts.

[Since the inspection took place AGS indicated that it will process requests for AGS CCTV received under a Section 4 Data Protection Act access request subject to the applicant indicating the existence of CCTV in a particular location].

12. Garda Vetting System

12.1 Garda Central Vetting Unit

The Garda Central Vetting Unit is made up of units that include the Garda Central Vetting Unit, the Garda Criminal Records Office and the Data Protection Processing Unit. These units are in the same location in Thurles and under the control of the same Superintendent. Garda Central Vetting Unit conducts a range of activities namely: overall records management; garda vetting; and responding to access requests made under the Data Protection Acts.

The Garda Central Vetting Unit currently has a staff cohort of 94 persons. Four of these staff are uniformed Garda members and 90 are civilian personnel. 18 of these staff are based in Ennis and were transferred to the GCVU as part of a civil service redeployment scheme. The Ennis-based staff conduct initial batch processing of vetting applications and their work is collected by an Ennis based staff member on Monday morning and returned on Friday evening.

12.2 Vetting Procedures

The Garda Central Vetting Unit (GCVU) conducts Garda vetting for organisations who must in the first instance already be registered with the GCVU. AGS outlined that garda vetting is conducted in respect of personnel working in a full-time, part-time, and voluntary or student placement capacity in a registered organisation, through which they have unsupervised access to children and/or vulnerable adults. In such cases, vetting is mandatory under legislation such as the Child Care Act 1991, the Child Care Regulations 2006 and the Teaching Council Act 2001. Vetting also takes place in relation to certain state employees working in sensitive areas and vetting has also been extended to persons working in the private security industry which are covered by the Private Security Services Act 2004 (nightclub security staff etc).

Despite specific legislation requiring vetting in various sectors, AGS stated that there was currently no legislation underpinning the Garda vetting process and so vetting was conducted on the basis of consent having being provided by the individual being vetted. However, the Team noted that the National Vetting Bureau Act was enacted at the end of 2012 and was expected to be commenced in the near future.

Garda Vetting is conducted only on behalf of registered organisations and their nominated ‘authorised signatories’ - the individuals who are administering the processing on behalf of the organisation. Vetting is not conducted for individual persons on a personal basis. Organisations apply to be registered with the GCVU and if provisionally approved, the organisation is invited to attend a mandatory training day. At the end of this training day the ‘authorised signatories’ from each organisation sign the final application and are allocated a registration number to be quoted on each application. In addition, the authorised signatory’s signature(s) is collected and is subsequently scanned into the GCVU system to be cross checked each time a vetting application is made. AGS informed the Team that large organisations, such as the HSE, would have more than one authorised signatory. It is also the case that certain organisations with low employee numbers may channel their vetting applications through an umbrella organisation such as the National

Recruitment Federation. However, AGS stated that each individual organisation will be registered with AGS.

AGS informed the Team that each authorised signatory is Garda vetted and if an issue arises with them, or the organisation they are conducting vetting on behalf of, they may be debarred from becoming an authorised signatory. However, AGS stated that in such instances, it gives the individual a right of reply and if the issue cannot be resolved at that stage, AGS will inform the organisation accordingly.

AGS outlined to the Team that the actual processing of vetting applications is carried out on a batch system. Applications are batched by AGS as they are received, while some large organisations send in applications pre-batched. The Team sat with AGS staff members processing vetting applications.

The first stage involves a staff member carrying out a visual check to ensure that all mandatory fields were completed as well as checking that the signature on a batch from an organisation matched that on the GCVU system for the authorised signatory. The Team was informed that in relation to date of birth (DOB), authorised signatories are required to verify that the date entered is correct. The staff member then enters the name, DOB, current and previous addresses and any alternative names supplied onto the system **"AGS Reporting Service"** (this system extracts information from PULSE and presents it in a user friendly form to the GCVU.) The system then presents matches and close matches for the information entered. The staff member then examines the matches to see if there are any relevant traces on the PULSE system to form the basis of a disclosure to the employer. If this is the case, these are printed off and attached to the application. The Team was informed that the system also has the facility to carry out reverse name searches.

It was noted during this process that all vetting disclosures are stored on a central drive which is accessible to all staff in the GCVU in case of future issues arising in terms of the content of the disclosure. The Team noted this is a departure from previous practice where only a summary record was kept. The ODPC is supportive of AGS keeping such a record in secure conditions as it removes the need for the organisations themselves to also store such information in what will often be less secure conditions. This is reflected in this Office's guidance on vetting.[28] However, the central drive does not provide a means to restrict access or examine access by particular staff members and it is therefore expected that this system will be replaced by a secure system that restricts access in line with business need and that allows monitoring of such access.

The Team was informed that PULSE entries created in respect of pre 2003 incidents may only include basic information but may contain a "Dublin Criminal Records" (DCR) reference. These are hard copy records stored in GCVU Thurles and referred to where necessary by GCVU.

The Team observed that matches or close matches returned in response to a search under the details supplied include matches where the individual may have been a witness or may have reported an incident. In one such example viewed by the Team, the applicant was a social worker and a match was returned in relation to an incident she reported to AGS in her official capacity. While it was not immediately apparent to the Team that the individual concerned was only involved in this matter in her professional capacity, the GCVU team member who was more familiar with the

28

http://dataprotection.ie/viewdoc.asp?m=m&fn=/documents/guidance/EmployeeVettingGuidance.htm

system stated that such a trace would be disregarded by the GCVU. ODPC considered that the GCVU PULSE extract systems should be programmed to not return such matches in response to a search to eliminate the possibility of any such traces being disclosed inadvertently. In addition, this will considerably reduce the number of traces being returned and accordingly make the examination for traces returned more relevant.

AGS submitted in response that the current functionality that returns all PULSE incidents should continue to work in this fashion. Reports are examined by trained staff who are very familiar with the system. Reports are manually checked to ensure that all relevant information is retrieved and nothing is inadvertently overlooked. The incident narrative will explain the connection of the person to the incident.

Following batching and checking by the GCVU, all vetting forms are referred to the GCVU Quality Control Section. All applications with a trace printout are quality checked and in addition, circa 10% of applications are quality checked by a team of six people. The Team observed this section checking under spelling of names, maiden name etc. The section keeps a note of all errors found and follows up with the individual where necessary. In addition, the Team was informed that regular mail shots are issued to all staff to highlight common errors. The Quality Control Section also quality check all disclosure letters and the Team was informed that GCVU has reduced the number of staff issuing disclosure letters to employers and have found that this has improved the quality of the disclosure letters issuing.

12.3 Pulse Update Section

Following quality control checking and in cases where it is not possible to establish the definitive position from PULSE, certain vetting applications are referred to the **Pulse Update Section** of the GCVU. The Team was informed that this section contacts the District Office of the station which would have originally generated the PULSE record under query to clarify the position with regard to the current status of the PULSE record. In cases where a reply is not received, a communication issues to the Superintendent in the station concerned.

The Team met with the two Garda Sergeants who have responsibility for examining all potential disclosures and was informed that of the approximately 6,000 vetting applications received each week, 20-25% would have some category of trace on PULSE. Of this group, AGS estimated that in the region of 25% of all applications generating a trace will be eliminated immediately due to filtering on the individuals' name, address and DOB data. The Team was informed that in serious cases where identity is in doubt, the matter is referred to the local Garda station for verification of identification and that this is always the case where any doubt exists concerning a sexual offence.

The Team examined a case where a PULSE record created in 2005 had not been updated to indicate the outcome of the investigation. Following receipt of a query from the **Pulse Updated Section** the record was updated to "Probation Act-non conviction". The Team was also shown a PULSE entry from 2003 referring to an individual accused of being intoxicated in a public place which read "Conviction-order to be affirmed".

The Team was also shown the example of a female with a drink driving charge where the forename, address and DOB were a match on PULSE but the surname differed. This was referred to the local Garda station for verification as it was considered the

individual concerned may have been married since the conviction and had not supplied her maiden name on the vetting application.

The Team viewed another example where a rape charge was recorded against an individual in 1995 but the outcome was not recorded on PULSE. The relevant Garda member concerned had been contacted by the PULSE Update section and recalled that there was a conviction, but there was no trace of the original file. AGS outlined to the Team that a Garda Sergeant was currently searching thorough court records in an effort to ascertain the court outcome. AGS indicated to the Team that such tasks are a daily occurrence at GCVU with operators encountering multiple incidents as outlined where clarification and checking was required in order to amend/update records.

The Team was also informed that a particular problem can arise where a case is appealed from the District Court. The primary court outcome types for recording an appeal on PULSE are "Appeal Allowed", "Appeal Not Allowed" and "Appeal Variation". AGS clarified that the court outcome type of 'Appeal Variation' on PULSE is used to record where the penalty imposed on the defendant from the original conviction is varied by the appellate court. The conviction still stands but the original order or penalty imposed has been varied. The ODPC recalled a case study in the 2000 Annual Report of the Data Protection Commissioner concerning this issue where the complainant's conviction at the District Court had in fact been appealed to the Circuit Court, and, whilst the conviction had been upheld, the sentence had been varied. These facts were not reflected in the record maintained by An Garda Síochána. When these facts were brought to the attention of An Garda Síochána, prompt action was taken to append the relevant Circuit Court details to the existing District Court data[29].

The Team noted that on the electronic reporting of outcomes side, the Criminal Justice Integration Project (CJIP) feed into PULSE classifies the court outcomes as either successful or unsuccessful. The Team was informed that this mismatch of reporting terms can cause difficulty with the accuracy of court outcomes on Pulse.

Another example viewed by the Team was of a "Simple possession of drugs charge" nine years ago where there was no charge or summons and where the individual was still classed as a 'suspected offender'. Again, this was referred back to the garda station concerned. The ODPC is aware that these details would not be disclosed as part of a vetting request if subsequent enquiries established there were no charges pressed or summons issued. It considers that if the individual to whom this record pertains made an access request under section 4 of the Data Protection Acts they would likely receive a copy of this record. The Team considered it is likely a caution at least was issued and if checking back with the garda station indicated a caution was issued under current disclosure procedures it would not be disclosed as part of a vetting check. However, if it was established that there was a court appearance in relation to this incident, the court outcome would be disclosed as part of a vetting check.

AGS stated that GCVU/GCRO/DPPU received a total of 327,903 vetting applications during 2012. Of this number approximately 20% had a trace. AGS outlined that the scrutiny of these vetting applications resulted in approximately 15,000 requests sent per annum via the PULSE Update Section to Districts to update/amend PULSE.

[29] http://www.dataprotection.ie/docs/Case-Study-1-00-An-Garda-Siochana/130.htm

The ODPC considers this is a high percentage relative to the proportion of the population who are required to be Garda vetted but welcomes the continued deployment of time and resources in ensuring records on PULSE are updated. The issue of the accuracy and completeness of records on PULSE is one of extreme concern to the ODPC. While the practice since 2008 whereby the CJIP system automatically populates PULSE with court outcomes at District Court level is to be commended, a problem may exist with records which don't fall into this category (such as Circuit Court outcomes). In cases where an incident proceeds to court it does not appear that AGS has any system to track that the record had been completed, insofar as possible, given available information at that time. It is noted however during the inspection of Mullingar, AGS Mullingar stated that the Sergeant present in Court has responsibility for recording the outcomes accurately onto PULSE.

Since the audit took place, AGS informed the Team that new procedures have been introduced in relation to the recording of Court Outcomes that are not transmitted electronically from the Courts Service. 'Case Supervisors' have been appointed within AGS who are now responsible for the recording of the result on PULSE in respect of all trials before the Circuit and Higher Courts. In addition, new functionality has been requested to assist in identifying any cases when a 'Final' court outcome has not yet been created where a case has been sent forward for trial. The ODPC welcomes the introduction of these new procedures.

The ODPC fully recognises that the nature of police work effectively means that investigations may continue for some time and that categories such as "suspect offender" may remain the correct categorisation for as long as the record is retained on PULSE. As previously outlined by AGS, if they consider there was sufficient admissible evidence to warrant recording the incident as detected and having been committed by that person they will allocate the role 'suspected offender' to an individual. If an ensuing court case was not successful due to insufficient evidence the role of 'suspected offender' would remain on PULSE. In addition, the Team clarified with AGS that if a case is struck out in court the individual concerned will still remain classified on PULSE as a 'suspected offender' – for example if a driver was detected by AGS driving erratically, the driver gave a false name and had no insurance and failed to produce it subsequently – then they will remain 'suspected offender' even if the case and all of the charges were subsequently struck out in court on a technicality. AGS reiterated that in the example above, the individual will remain as a 'Suspected Offender' in the incident as there is a reasonable probability, based on sufficient evidence, that the individual did commit the offence. The Court Outcome will reflect the fact that the case was struck out in court (i.e. the individual was not convicted of any offence).

AGS confirmed to the Team that the 'role' of the person within that incident may be changed to reflect that the individual is no longer a suspected offender in some instances e.g. a court outcome where a person is acquitted.
The ODPC observed that while there is a comprehensive review system in place in GISC to review PULSE records when initially created, it did not consider there was an established policy or system to review PULSE records on an ongoing basis. An individual who is the subject of a vetting check or an individual who makes an access request under the Data Protection Acts will as part of procedures in place have their record checked if there is a doubt as to their identity or the final outcome in relation to how the incident is recorded on PULSE. Aside from these instances, the ODPC recommends that AGS put in place a records management programme to systematically review and check the accuracy of PULSE records on a rolling basis.

This is essential to ensure that the categorisation of individuals and incidents on PULSE reflects the most current status in relation to the incident recorded.

In addition, all records detected on PULSE which are inconclusive if charges were pressed should be followed up as a matter of course if encountered by members as part of their normal investigative duties.

12.4 Garda Vetting Disclosures

The ODPC considers that a fundamental area requiring clarification by AGS to data subjects is to outline clearly what will be disclosed back by AGS via an authorised signatory to an organisation for vetting purposes as opposed to what a data subject can expect to obtain a copy of via a subject access request made to AGS. This is the source of frequent enquiry to this Office when a data subject or their solicitor makes an access request to AGS and views the content supplied in response by AGS.
For example, a response to an access request by AGS might contain three pages of records regarding the individual where they could be classified on PULSE as both 'suspected offender' and 'witness' and various other roles. In addition to the listing of such entries, a copy of any court outcomes recorded on PULSE will also be supplied to the individual as part of the access request response.

AGS confirmed to the Team that only court outcomes will be disclosed by AGS as part of a vetting check under current procedures. Based on the level of queries to the Office, we conveyed to AGS our view that the general public are patently unclear regarding this distinction and may be unnecessarily concerned by the data supplied in response to a section 4 access request, when in reality under the current vetting regime it would never be disclosed as part of a vetting check.

In addition, despite guidance issued by the ODPC in term of disclosures, members of the public do not appear to be aware that court cases that resulted in non-conviction or were struck out **WILL** be disclosed as part of a vetting disclosure. Indeed under the proposed new procedures once the National Vetting Bureau (Children and Vulnerable Persons) Act has commenced the ODPC understands that 'soft' information may also be disclosed in certain circumstances such as adult cautions or instances where proceedings in relation to a sexual offence are dropped.

The disclosure of all court outcomes is highlighted in guidance issued by the ODPC:

> **b) Information that may be released as part of the vetting process**
>
> When a vetting subject gives their written permission for An Garda Síochána to disclose details of all prosecutions, successful or not, pending or completed and/or details of all convictions, recorded in the state or elsewhere in respect of them to a registered organisation, all such details as held on record by An Garda Síochána in respect of the vetting subject are disclosed. In the case where vetting subjects have been prosecuted, notwithstanding the court outcome in respect of the prosecution, the factual details contained in the resultant court outcome are disclosed to the authorised signatory[30].

[30] http://www.dataprotection.ie/docs/Guidance-Note-on-data-protection-considerations-when-vetting-prospctive-employees/1095.htm

12.5 Non-Convictions, Old or Minor Convictions

The ODPC considers that the possible disclosure and indefinite retention of information about non-convictions or old or minor convictions is not in accordance with the spirit of requirements under the Data Protection Acts. The ODPC accepts that AGS has no legislation to adhere to in this regard as currently Irish legislation makes no provision for "spent" convictions.

The ODPC is also aware that since the inspection took place that the National Vetting Bureau (Children and Vulnerable Persons) Act has in fact not commenced due to an issue with the Criminal Justice (Spent Convictions) Bill 2012 which is now stalled at Report Stage in the Dáil. The Minister for Justice Alan Shatter stated in a written response to a parliamentary question in May 2013 that

> "the Bill is intended to work in harmony with the National Vetting Bureau (Children and Vulnerable Persons) Act 2012. However, elements of that Act concerning the disclosure of convictions are under review at present having regard to a recent judgment of the UK Court of Appeal in (On the Application of) T and others v Chief Constable of Greater Manchester [2013]. The Court considered the circumstances in which it is appropriate to disclose convictions for minor offences with particular regard to Article 8 of the European Convention on Human Rights. While the judgment concerns legislation that differs from the 2012 Act and the proposed Bill, I take the view that the legal principles identified by the Court in relation to the application of Article 8 merit consideration. In the event that some modifications are required to the 2012 Act my intention is to bring them forward by way of amendment to the Bill and to make any consequential changes to the Bill itself that are required to ensure that the two regimes work in harmony. Until this work is complete I am not in a position to give an indication of the likely timing of Report Stage. However, I am conscious of the importance of the Bill to the reintegration of offenders and I will endeavour to ensure that there is no undue delay[31]."

The ODPC expects that all imminent legislation such as the National Vetting Bureau (Children and Vulnerable Persons) Act and the Criminal Justice (Spent Convictions) Bill 2012 will provide for a comprehensive system where safeguards are introduced in relation to the disclosure of old and minor convictions or the disclosure of non-conviction information. The ODPC continues to be available to offer guidance on the data protection issues which may arise.

Overall, it is recommended that a policy framework and guidance should be drawn up by AGS outlining the circumstances in which all disclosures for vetting purposes will be made under forthcoming legislation with a clear framework outlining the range of what may be disclosed and in what circumstances and the exact time period under which non-convictions and old or minor convictions may become 'spent'.

13. Processing of Data Access Requests

The Garda Central Vetting Unit (GCVU) is also responsible for the processing of all requests for personal data under Section 4 of the Data Protection Acts. The Unit received 11,266 such applications in 2012. The Team was informed that apart from

[31] **Wednesday, 22 May 2013 Dáil Written Answers Nos. 204 - 211**
http://oireachtasdebates.oireachtas.ie/debates%20authoring/debateswebpack.nsf/takes/dail2013052200087

personal information available on PULSE, GCVU holds no other personal data and is entirely dependent on individual Garda stations to supply such data if there is, for example, an incomplete outcome indicated on the PULSE record. The Team was informed that there can be considerable delay in receiving a response from Garda stations and the GCVU is often forced to enter into protracted communications with Garda stations to obtain the information required for release to the requestor.

The Team noted that **HQ Directive 95/2012 – Data Protection in An Garda Síochána** sets out the responsibilities of AGS in regard to access requests and states, inter alia, that all such requests received at any Garda Station or at any Office of AGS must be forwarded to the GCVU. In addition, this directive states that all information relating to the person must be forwarded to the GCVU 10 days before the 40 day limit in order for the material to be assessed for a decision to be taken on its disclosure.

The ODPC considers that the publication of the HQ Directive referred to above strengthens the position of the GCVU on this matter to allow the organisation to meet its responsibilities in this area.

To further address issue of delays in processing access requests, it is recommended that this wing of the GCVU be adequately resourced to deal with data subject access requests. As an organisation, AGS needs to instil within each garda district a culture of compliance with the 40 day statutory requirement in terms of the processing of access requests and in terms of the HQ directive which seeks adherence to this statutory requirement.

[AGS stated that this recommendation is receiving ongoing attention]

In addition, it is recommended that all access requests made by former or serving members are processed in a dedicated queue separately within AGS.

The ODPC is also cognisant of the high number of access requests cited by AGS and the provision in the Data Protection Acts 1988 & 2003 which has not yet commenced - Section 4 (13).

As per advice featured in the **'Guidance Note: data protection considerations when vetting prospective employees'**

> "it is a clear abuse of the right of access for an employer to attempt to require a prospective employee to reveal the result of such an access request. This Office considers that such practices constitute a breach of the Acts as the consent given cannot be considered to be free. Furthermore, any such action by an employer will be a criminal offence when Section 4(13) of the Data Protection Acts comes into effect".

This is an area to be monitored closely by this Office in conjunction with the co-operation of AGS.

The Team noted the section 4 access request form is readily available on the AGS website as follows:

What is the procedure for seeking access to my personal data?
An individual seeking access to their information should complete a Data Protection Access Request form - F2032 and return it with relevant enclosures to the Garda Criminal Records Office, Racecourse Road, Thurles, Co. Tipperary.

[32] http://www.garda.ie/Documents/User/Data%20Protection%20F20%20-%20Nov%2012.pdf

The Team during the course of its dealings with AGS noted the standard AGS response to a section 4 data subject access request (in terms of data eligible for release under the Data Protection Acts) is in the format of the following example:

PERSON SEARCH

Name	**Date of Birth**	**Location**

Incident Date	**Incident Category**	**Incident Location**	**Role of Data Subject**
22/05/2008	Burglary	Main street, Navan	Injured Party

Incident Date	**Incident Category**	**Incident Location**	**Role of Data Subject**
14/10/2008	Attention & Complaints	High Street Dundalk	Witness

Incident Date	**Incident Category**	**Incident Location**	**Role of Data Subject**
11/12/2012	Public Order offences	Village X, Co, Co. Dublin	Suspected Offender

Incident Date	**Incident Category**	**Incident Location**	**Role of Data Subject**
01/01/2013	Traffic	Village X, Co. Dublin	Suspected Offender

Court Outcomes

Date:	**22/03/2013**
Court:	**Circuit Court**
Charge:	Intoxication in a public place Threatening/abusive/insulting behaviour in a public place Assaults causing harm
Result:	Non- Conviction – Appeal allowed

Date:	**01/04/2013**
Court:	District Court 43
Charge:	Exceeding Special Speed limit 60 km/h
Result:	Conviction Fine 150

We noted that previous access request responses provided an additional column of data headed 'Details'. We enquired whether a formal decision had been taken by AGS not to provide this information anymore. AGS in response stated that if details are available they are generally disclosed.

In terms of what may or may not be provided by a local garda station from manual files (statements made by a data subject etc) this is an area requiring further

clarification. We recommend that GCVU in acknowledging an access request, explain that their response will be based primarily on what is held on PULSE and if further information is sought it is a duty on the data subject, imposed by the DPA, to assist in indicating where the relevant personal data may be located.

In terms of factual errors or cases of mistaken identity, AGS confirmed that it would be the responsibility of the data subject to engage with AGS to review the record as the same in-depth checking procedures are not in place for subject access requests as for disclosures for vetting purposes. Whilst these procedures to amend/rectify data held on PULSE are in operation, the ODPC is also aware of how AGS outlines to data subjects the position of AGS in relation to section 6 requests to amend data held on PULSE where AGS believe the existing entry is factual and correct. This will be communicated to the data subject in a manner similar to the following:

> **1.** "the data in relation to you pertaining to the incident on… was recorded for the purpose of keeping an accountable organisational record of the action taken by AGS in relation to the incident. This was in line with standardised recording procedures on the Garda computer system PULSE, for recording incident types, the role of individuals within incidents and subsequent actions and outcomes, if applicable to the incident."
>
> **2.** The record in respect of this incident was generated by operational members of AGS in the performance of their legitimate policing function of preventing, detecting or investigating incidents where offences may be disclosed. This record has not been deleted as it is a factual representation of the action taken by AGS in respect of this incident.
>
> **3.** The position in respect of data kept by AGS in respect of incidents is that all files containing such data are made or received within the course of the business of AGS. This being the case, the data contained in all such files forms part of a Departmental Record within the meaning of section 2 of the National Archives Act 1986. AGS is a scheduled body within the meaning of Section 1 of the National Archives Act 1986 and is, therefore legally obliged to retain and preserve Departmental records made in the course of its business. This being the case, Departmental records in respect of data kept in incidents are retained and preserved in AGS, pursuant to Section 7 of the National Archives Act 1986.

14. Exchange of Data with Other Countries

The Audit did not include an examination of all exchanges with EU and other countries under legal provisions such as the Criminal Justice (Mutual Assistance) Act 2008, Garda Síochána Act 2005 or the Europol Acts. However, the Team did examine AGS involvement in the European Criminal Records Information System (ECRIS).

14.1 ECRIS (European Criminal Records Information System)

The computerised system ECRIS was established in April 2012 to achieve an efficient exchange of information on criminal convictions of EU nationals between EU countries. ECRIS is based on a decentralised IT architecture: criminal records data is stored solely in national databases and exchanged electronically between the central authorities of EU countries upon request. The EU country of nationality of a person is

the central repository of all convictions handed down to that person. The country's authorities must store and update all the information received and retransmit them when requested. As a result, each EU country upon request is in a position to provide, to another EU country, up-to-date information on its nationals' criminal records.

AGS outlined to the Team that the legal basis for ECRIS is the Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States. AGS clarified to the Team that the relevant implementing legislation in this regard was the Criminal Records Information Systems Bill 2013 which is currently at draft stage in the Oireachtas. The ODPC recommends that this legislation be passed as soon as possible in order to underpin the legal basis for the operation of ECRIS.

AGS stated that the Criminal Records Office is responsible for the operation of ECRIS on behalf of AGS.

The Team was informed at the time of the inspection that ECRIS was live with interconnectivity achieved with nine other countries using the system: Romania; Estonia; Austria; Latvia; Netherlands; Lithuania; Denmark; Finland and Poland. Since the date of inspection full interconnectivity has been achieved with the following additional countries; Bulgaria, France, Czech Republic, Hungary, Belgium, United Kingdom, Spain, Cyprus, Greece and Slovakia.

AGS clarified the exchange is only for criminal purposes. The Team viewed a request from Lithuania to Ireland for court information. The Team was informed that in such a case, the request would go to the investigating AGS member. The query was shown as having been completed.

The Team was informed that AGS must be entirely satisfied that it has identified the correct individual prior to releasing any information through the ERCIS system, information relating to close matches will not be released.

AGS stated that it has not yet commenced the process of sending to other member states convictions relating to their nationals' in Ireland. AGS stated that it's IT Division is currently working on a system which will extract the relevant information from PULSE and send that information through the ECRIS system which has an automatic translation facility.

AGS stated that some ECRIS members have proposed that the ECRIS system be extended in order that it can be used for vetting purposes. The Team was informed that some such requests had been received citing child trafficking legislation. AGS stated that it has not responded to such requests to date.

15. Data Security: IT Security

15.1 Overview

At the commencement of the inspection, the Team was given a comprehensive presentation by AGS on their IT and Communications systems and was referred also to HQ Directive 118/09 which outlines An Garda Síochána's Security Policy for the Use of Information and Communications Technology including portable data devices and the transfer of electronic data.

The Team was informed that the Garda IT network has circa 16,000 domain users and this number is decreasing due to the lack of recruitment and rationalisation of Garda stations. AGS IT Unit supports approx. 9,000 desktop machines, of which 6,518 are networked, 1,100 servers and 2,200 network printers.

In relation to networking, AGS stated it is their intention to network its entire system however, current financial constraints essentially mean this will not happen in the short term. While the PULSE and Garda email systems are networked, there is no central document management system to deal with investigation files and all other routine correspondence.

15.2 Topology of system

AGS informed the Team that it operates a hub and spoke topology. Connection between Garda Headquarters (GHQ) core network and the various sites such as local stations and the airports is via an encrypted Virtual Private network (VPN). There are currently 400 AGS sites and 25 third party sites.

15.3 Security of IT Equipment and Infrastructure

The Team was informed that Garda ICT section issue official laptops and USB drives and that all these are encrypted in line with HQ directive 118/09. This directive states, inter alia, that "only Information and Communications Technology equipment supplied by the ICT Division and /or Procurement section of An Garda Síochána shall be used".

15.4 Laptops

AGS informed the Team that there are currently 1,200 laptops issued to members of AGS. The laptops are issued at a regional level to Inspectors and above. The laptops are provisioned by AGS ICT Unit and issued to Assistant Commissioners/Executive Directors for use within their area of responsibility. The Issuing Officer is required to maintain a list of users to whom such equipment is issued.

AGS stated that the laptops are encrypted.

AGS informed the Team that it is currently working on developing a locked down laptop with secure access to AGS systems. As part of this system they hoped to develop a docking system for laptops but stated that delay in updating information immediately after docking may cause a problem.

15.5 USB Devices

AGS issue encrypted USB devices.

AGS stated that USB device are only supplied on a business needs requirement. AGS issued instructions to its members via HQ Directive 118/09 which issued in August 2009 that the use of non-AGS provided USB devices must cease.

The Team asked if AGS could verify whether any personal data was stored on personal laptops, PCs or unencrypted USBs. AGS stated that while members have been informed that it is against official policy in this area, they cannot give a 100% guarantee to this effect.

The Team enquired whether PC access for USB drives was locked down to ensure that only encrypted USBs were used and were informed that this is not currently the case. The ODPC recommends that PCs are locked down against USB access by default and access by a USB drive should only be allowed on a case by case business need.

15.6 Remote Access to the Garda System.

'The Team was informed that smart phones are issued to members of the rank of Superintendent and above. 'Smart phones can be issued to members below the rank of Superintendent where an application has been made supported by an appropriate business case for the issue of a smart phone. These applications are dealt with on a case by case basis. 'Smart' phones are used as an ordinary phone and to send and receive the individual's Garda email.

All garda-issued smart phones can connect over a secure encrypted VPN into the organization for email access only. The data is encrypted and access to external email can be disabled if a device is reported lost or stolen. Similarly, Garda email can be accessed from an external laptop or PC using logon credentials and a RSA PIN code. Remote access to email is restricted by grade with only Inspector upward having such access. AGS informed the Team that, where a member has remote access, access is limited solely to e-mail. There is no remote access to PULSE or any other Garda system. AGS indicated to the Team that it is working on a pilot of secure remote access to Garda Information Systems using a Garda issue device which is ongoing during 2013. Secure Remote access to email is available.

Tetra radios are issued to operational members and are primarily used for 'Group' communications. Tetra radios can be used to contact certain phone numbers (E.g. GISC). The issuing of a tetra radio is separate to the issue of a phone.

15.7 Network Security

The ICT Unit is divided into two areas, Telecommunication Section and ICT Unit. The Telecommunications Section maintains the outside perimeter of the network, what was referred to as the Castle Walls, and ICT are responsible for all areas inside the Castle Walls.

The Telecommunications Section within AGS maintains the inward/outward facing connections to the AGS network. The Team visited the offices of the Telecommunications team and were shown the network monitoring tools in use by the team. AGS informed the Team that there is a 24/7 monitoring of the network in place and alerts are issued via e-mail to a member of the Team. AGS demonstrated to the Team the various firewalls in place to protect the AGS network. AGS also informed the Team that the Telecommunications Team maintain their own network equipment, separate to the internal network devices to prevent a duplication of potential errors.

AGS informed the Team that the patching of perimeter devices takes place on a monthly basis and internal devices are patched on a quarterly basis. Where a critical alert is issued, immediate actions are taken.

AGS outlined to the Team that the National Digital Radio Service was procured by the Department of Finance to provide a managed nation-wide digital radio services for voice and data purposes to all public security and emergency services and non-commercial public bodies in the Irish public service. This contract was won by TETRA Ireland. This in effect means that TETRA Ireland, meets all the necessary

contracted network infrastructural costs, such as construction of masts, installation of antennae and network hardware.

Garda Telecommunication's role is to procure TETRA terminal equipment to equip the Garda resources such as personnel, vehicles and Control Rooms, and to manage the configuration, operation, maintenance, security and billing of this equipment through its lifecycle.

AGS IT Security monitor system activity and traffic flows, the Team was informed that AGS consider an in-house accidental attack to be a much higher risk than an external attack.

15.8 Desktop Device Security

AGS informed the Team that there are approximately 9,000 desktop devices in operation. Networked desktop unit are pre-configured by ICT for use in the various locations.

The networked desktop devices are configured to lock after 10 minutes of inactivity, requiring the user to enter their network password to re-access the system. AGS informed the Team that in the Airports, the desktops are also configured to lock after 10 minutes of inactivity but are also configured to automatically log-off the network after a further 20 minutes.

15.9 User Accounts

The Team was informed that requests for account creation/modification to the AGS IT systems is made via two forms, ITSU1 and ITSU2. ITSU1 is used for general system access and ITSU 2 is used for exceptional user access e.g. grant a CIO access to create or update intelligence records. Permissions are based on rank and role. Gardaí and Gardaí reserves' access is rank based. Civilian access is grade based and certain permissions are role based e.g. Criminal Intelligence Officer.

ITSU 1 form is sent up by the Garda College to IT Security for all joiners. A password is assigned and has to be changed on initial log on by the member.

The ODPC requested further details from AGS regarding the strength, complexity and duration of the password and asked AGS to confirm it is at least in line with security guidance issued by this Office.

AGS stated to the Team that this password is issued in hard copy form in a sealed envelope to all joiners when they are leaving the Garda college. AGS stated that if a student Garda does not graduate, their account is disabled. In this regard, there is no rationale for not deleting the account of a student Garda who does not graduate and this Office recommends that such accounts should be deleted rather than simply disabled.

In respect of movers/leavers, IT Security keep the Garda Active Directory up to date by tracking HR bulletins which issue 14 days before transfers are due to take place. When a user moves District, a user provisioning tool is used to remove that user from all non-standard groups and the user will have to reapply for any additional access required.

The Team reviewed the code used in the provisioning tool to determine the actions being carried out in the cases of a new member, a member moving location / grade and a member retiring from the force. The Team was unable to see the provisioning tool in action as the visit occurred between issues of the HR bulletins and the last bulletin had already been acted upon. The Team was satisfied that the provisioning tool performed the requisite changes as expected. It is noted by the Team that when a member leaves AGS, their account is not deleted. The user account is removed from all groups and the account is disabled. AGS informed the Team that the account is not deleted so that it can be associated with queries run in Pulse at a later date, if necessary.

It was noted that previously the ITSU form was faxed or posted to the District office, collected by the IT Security team, scanned, renamed and sent to the ITSU Section mailbox. However, the Team was informed that a new process is now in place whereby the District Clerk can scan the form and email it to the dedicated ITSU mailbox. The Team was informed that IT Security processed 8467 ITSU forms in 2010, but year to date has only processed 5147 forms, due to the drop in recruitment.

15.10 Roles and Permissions

Members are assigned access to the various systems, including printing facilities and software access, through Active Directory (AD).

The Team looked at the permissions assigned to a CIO which required membership of 24 groups within AD. A Garda based in Monaghan was a member of 13 groups within AD.

The Team examined the administrator accounts within AD. The Team found a domain administration account which was used to assign roles to particular machines and a separate administration account populated with staff members. This particular administration group contained 4 individuals listed and several groups also nested in the account. Upon examination of these groups, which involved Operations Directorate and Service Management, the Team found a further 32 individuals were being granted administrator access to the domain. This fact was highlighted to AGS on the day of the inspection and the Team sought further investigation into the level of access to the administrator account. Since the audit took place AGS indicated that its IT Security section has investigated this issue and subsequently reduced the number of administrator access users to 14. AGS IT security also stated it is continuing to carry out operational testing with a view to further reducing this number. Regular reviews will be carried out on the need for such access in the future to ensure that only the minimum number of users have such access and have a valid business requirement for such access.

The Team also noted the difference between various user roles within PULSE. The Team examined the difference in access between the roles of CIO, E.O and E.O Reserve. These were test accounts set up for the visit of the Team. The Team noted that the CIO was the only user with access to the “Intelligence” and “Items of Interest” functions within PULSE. The Team also noted that in each menu option, such as Create, Maintain, Actions, Reports etc, the CIO user had a greater number of options available to it.

The Team also noted that in comparisons between the E.O and E.O Reserve users, the E.O. Reserve had limited functionality in comparison with the E.O. user.

15.11 Password Security

As outlined above passwords are assigned to new users by the training college and must be changed at first log in.

There is a self service facility on the Garda Portal whereby a user can register answers to a number of security questions which can be used to issues them with a new password if they cannot remember the original password allocated. New passwords can also be allocated by the IT helpdesk who must satisfy themselves as to the identity of the caller. This is done using Active Directory where staff details are stored under their registration number. In addition the helpdesk can verify ID by checking if a caller is in a group, but the helpdesk cannot make an addition to a group.

15.12 IT Helpdesk.

AGS operate an IT helpdesk at Garda HQ. This helpdesk is staffed by a combination of civilian staff, contractors and Garda members. The contractors only have limited access to the system and no access to PULSE, although they can start the PULSE engine to ensure that it is running. The Team viewed the helpdesk in operation and tested the system where a contractor tried to access the pulse system. While the contractor could see the system was operational, an error 401 occurred when they tried to enter the PULSE system.

The Helpdesk can shadow users who report issues but the request to shadow must be accepted by the user.

The Team noted a report within the Helpdesk Office which identified the Top Ten calls received by the helpdesk team. The Team noted that the single biggest issue resulting in calls to the helpdesk was password resets which accounted for approximately 3,500 calls for the year up to the beginning of October.

15.13 Printing

AGS stated that it has 2,200 networked printers and there are also a number of stand alone printers in stations. It stated that it is moving to a “Follow-me’’ printing system which allows users to print to any supported network printer in a particular AGS location and then authenticate at the printer to retrieve it. The Team was informed that the information is held on the server and not on the printer/photocopier. In relation to where a document is photocopied, the data is stored on the hard drive. The team was informed that all such hard drives are securely destroyed when the printer reaches end of life.

15.14 Disaster Recovery.

AGS has two separate server farms, one of which operates as a disaster recovery site.

Access to each of the buildings housing the server farms is restricted to relevant personnel. All visitors are required to sign in when visiting the areas. The team

examined the visitor log books at both locations and found sufficient entries to show that the log books were being routinely used.

AGS informed the Team that data from the 126 networked servers is backed up to tape on a daily/weekly /monthly basis. When satisfied with the monthly back-up, daily and weekly back-up tapes are overwritten and monthly back-ups are retained indefinitely.

15.15 Waste Disposal

During the IT inspection on the 16th November, the Team came across a secure waste bin in the IT Building which was not locked. A Team Member was able to open the bin and access the documents contained within the bin that were due for shredding.

AGS responded to this stating that Access to the Garda HQ Complex and section buildings is strictly controlled at all times on a regulated structural basis to staff that are required to be in areas only as business requires. In the main, staff allocated to individual buildings only have access to those particular buildings and except for senior management do not have general access.

In terms of the issue itself, in Garda HQ, locked and secure numbered 240lt fully mobile wheeled carts are provided for the storage of confidential office paper waste in key locations throughout the GHQ Complex. In relation to the specific incident, all local senior management in sections are issued with a key to open the confidential bins in the event of a mistake in relation to a document mistakenly binned for shredding or its retrieval is required. This key is issued to senior management for this purpose and is not on general issue.

With regard to this particular issue, ICT indicated that it believed that the override key was used to retrieve a document or had been opened to allow a bulk disposal of documents and subsequently inadvertently left open. This is the first instance of this type in over 4 years, and can be viewed as a complete exception to the confidential waste destruction protocols in situ in the Garda HQ Complex. Management in the ICT block are aware of this incident.

16. Findings

Excellent co-operation was received throughout the inspection. The Inspection Team considered there to be a strong organisational awareness of data protection principles generally.

The processing of personal data is at the heart of police operations. Data processed by AGS is classified as sensitive data, requiring special protection, under both EU and national law. The safeguarding of all aspects of the processing of this information must therefore be a priority. In order to ensure a constant focus on this requirement, ODPC consider that data protection should be the responsibility of a dedicated unit, headed by a Data Protection Officer with a direct reporting relationship to the Garda Commissioner. The appointment of such an officer will in any case become an EU obligation if the draft Directive on data protection in the area of law enforcement, presented by the EU Commission in 2012, becomes law.

ODPC has addressed a number of specific recommendations to AGS, arising from the audit. These are listed at the beginning of this report, together with the AGS responses to them. In many cases, action has already been taken by AGS to address the issues raised.