THE CHIEF CONSTABLE OF CLEVELAND

General Data Protection Regulation (GDPR)

Internal audit report 7.22/23

Revised Final

2 November 2022

1. EXECUTIVE SUMMARY

Why we completed this audit

As part of the 2022/23 internal audit plan we have undertaken a review of the Force's data protection framework and its approach to compliance with the UK General Data Protection Regulation (GDPR) in relation to the use of personal data, including Part 3 of the Data Protection Act 2018 (DPA) in relation to the processing of personal data for preventing, investigating, detecting, and prosecuting crimes.

The Force utilises its Information Management and Data Protection Policy which outlines the underpinning procedures when collecting any data for which it is responsible, and it is expected to use the information in line with the legislative requirements and in pursuance of the Force's policing vision and aims. The policy acknowledges the roles and responsibilities across the Force from the Chief Constable to all employees to ensure that there is a consistent understanding on how to retain and dispose of information appropriately, lawfully and with confidence.

The Force currently has a dedicated Data Protection Officer (DPO) and Information Management Team (IMT) in place who are responsible for data protection across the Force and ensuring that all legislation and guidance is being adhered to. Whilst they are primarily responsible for these areas, information asset owners have been identified and are in place across the Force. Information asset owners are senior staff within the Force and are responsible for ensuring that the data assets they oversee are managed in adherence to GDPR and DPA 2018. Both the information asset owner and the IMT work collaboratively to identify new data assets. The GDPR Data Protection Auditor completes an annual review of the information within the Register of Processing Activities (RoPa) and the Information Asset Register to ensure that the details are still relevant and accurate.

Prior to our audit, the Force had conducted a self-assessment exercise using the ICO Self-Assessment Toolkit which had identified a number of areas for further development. In response, a request has recently been made and approved to recruit an Information Governance Manager to assist in progressing the outstanding areas highlighted. Recruitment was ongoing at the time of our audit.

Conclusion

As a result of our review, we have agreed **one high**, **two medium** and **two low** priority management actions. It should be noted that several of these actions stem from a lack of resources to complete the required day-to-day tasks to effectively monitor Force compliance with GDPR and DPA 2018 legislation and, as noted above, the Force is currently recruiting for an Information Governance Manager to assist in progressing the outstanding areas highlighted within the ICO Self-Assessment.

The Force has a RoPA in place, which is reviewed on an annual basis by the GDPR Data Protection Auditor. Each processing activity is required to be audited to confirm that the information is up to date and relevant. However, from the review of the RoPA we identified 72 processing activities which had not been reviewed within the annual audit cycle, and there was no evidence available within the audit history to suggest a review had been undertaken. The Information Asset Register is used to outline the information asset owners of data asset to ensure that data owners are aware of their responsibilities in relation to GDPR and DPA 2018. However, we noted that several of the asset areas did not have an asset owner documented within the register to take responsibility if a breach occurred.

Further details of these actions can be found under section two of this report.

Key findings

Following our audit testing, we have agreed one high, two medium and two low priority management actions:

In discussion with the DPO, we understand that the Force has already acknowledged they have further development to undertake in respect of consent. Completion of the ICO's self-assessment clearly highlighted that the Force requires additional work to manage consent and this has been a key development area within the last 12 months. The DPO made the decision to focus solely on one area to identify the needs and requirements before they consider the wider areas within the Force.

The DPO made the decision to focus on digital extraction consent as this was a known area which required consent, and is one of the areas where consent would be more frequently requested to support investigations.

As the DPO has previously implemented a guidance in relation to consent in her prior role, she is hoping to implement the same guidance within the Force to set out the expectations for when consent is required and what relevant information can be obtained. Within section 6 of the ICO Toolkit it is clear that further development needs to be completed in order to ensure that consent is obtained and managed appropriately. However, until the Information Governance Manager is appointed, there is no availability within the team for this level of work to be completed.

When resource is available, the Force will implement an action plan to outline all data asset areas across each department to ensure that there is sufficient focus on consent and ensuring that this is obtained and managed appropriately. **(High)**

We reviewed the Information Asset Register which outlines each data asset and the information asset owner. The IMT completes a new data asset record within the register when they are informed of such. If the team is not advised of a new data asset, it will typically be picked up in the annual audit review completed by the GDPR Data Protection Auditor.

Asset owners are identified by the individuals directly and report to the IMT. If there are changes to data guardians or asset owners, they are required to inform the IMT, if they do not inform the team, the information will not be picked up until the annual audit review. There are currently 17 asset areas which have not been allocated an asset owner within the Information Asset Register.

If asset owners or guardian changes are not identified on a timely basis, there is a risk that if a breach occurs there is no individual available to take responsibility and provide a solution. **(Medium)**

We reviewed the Force's website and confirmed that there is a Data Protection Act 2018 and UK GDPR Subject Access Request document published to inform individuals of their rights to request information on themselves or another person for the following:

- Disclosures for family court proceedings;
- Register sex offenders data (Sarah's Law); and
- Domestic violence offender data (Clare's Law).

The document clearly outlines how individuals are required to confirm their identity before any information is provided.

In discussion with the Information Rights Decision Maker, we understood that Subject Access Requests can be submitted by any means such as email, post, telephone, in person or via the .gov single online home platform. We also confirmed that the Information Rights Team is required to assess all information requested before disclosing any details to the individual. This is to ensure that there are no breaches for ongoing investigations and is only the information requested within the agreed parameters.

We confirmed with the Information Rights Decision Maker that they currently have no formal procedure document in place to set out the process for Subject Access Requests and deletion of data. However, we note that this had already been identified as part of the ICO self-assessment and included within the Force's GDPR action plan.

There is a risk without a procedure document in place, there is no consistency with responses to requestees, and they are unable to set expectations without an agreed timescales and decisions. **(Medium)**

For details of the remaining **two low** priority actions, please see section two of this report.

Our audit review identified that the following controls are suitably designed, consistently applied, and are operating effectively:

We completed a walkthrough with the GDPR Data Protection Auditor of both registers, Information Asset Register and the RoPA, which are stored within the Share Point system. From this exercise we confirmed that both registers are live working documents within the system and access is restricted to the IMT and the relevant asset owners and guardians.

We obtained a copy of the Force's Information Management and Data Protection Policy which outlines the roles and responsibilities across the Force. We noted for data discovery, Heads of Departments are responsible for identifying any new data assets and communicating this to the IMT so that it can make appropriate arrangements and add the required details to the Information Asset Register and the RoPA.

Once the data asset has been identified the purpose of the data processing is updated within the RoPA. Within the register we confirmed that there is a section which outlines the purpose of processing, and within each asset there are documented reasons for the processing of the data. A couple of examples from the register are: prevention and detection of crime, safeguarding, complaints, corruption within the Force, and management of staff. This information can be found within column 'I' on the register. We confirmed that the purpose for processing data was documented for all data assets within the register.

Through review of the RoPA which identifies within column AI the location of personal data. Within this box all systems and software are identified where the data is stored for each specific processing activity. These are some examples of locations where personal information is stored:

- Emails in relation to an investigation;
- Laptop / Hard drives;
- Webstorm;
- Y Drive;
- E-Duty;
- Niche;
- Police National Computer (PNC);
- Police National Database (PND); and
- SharePoint

Additionally, we identified that column “AJ” of the RoPA outlined the details of instances where the data is required to be transferred to a third party, this could be through the Internal Police Association, Interpol, or the Home Office. Within the register the reason for which data would be transferred, if necessary, is clearly identified.

The DPO has confirmed that they have formally been employed by the Force as the DPO. This has been acknowledged by the ICO and the Force’s ICO certificate has been updated to reflect this appointment. We have also confirmed that the Force’s website has the DPO’s name and contact details.

We reviewed a copy of the role profile and confirmed that the description of the DPO's role matched the work that the DPO is currently completing and that their experience matched the role responsibilities. We also noted the DPO reports to the SIRO who is usually the Deputy Chief Constable but it is temporarily the Assistant Chief Constable, as well as the Information Assurance Board and that the DPO is supported by a number of individuals in the IMT.

We obtained a copy of the Force’s Information Management and Data Protection Policy and confirmed that, within the document, all roles and responsibilities relating to data protection across the Force are outlined. The policy stipulates that the DPO is responsible for ensuring that the Force is meeting its data protection legislative obligations.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Area: Maintenance of the RoPA				
Control	The Force maintains a RoPA. The register is reviewed at least annually between the GDPR Data Protection Auditor and the information asset owners to ensure that information on data assets and owners is up to date and accurate and the register is clearly dated to reflect this review. Information asset owners have access to the register should updates be required in year.	**Assessment:** **Design** **Compliance**	 ✓ ×	
Findings / Implications	The RoPA is reviewed annually by the GDPR Data Protection Auditor with each asset owner to ensure that the relevant data is up to date and accurate. We reviewed the RoPA to confirm that the register is up to date with all relevant information. In line with the GDPR Article 30 all Registers of Processing Activities are required to identify the following: • Personal data - data subject categories; • Purpose - legal basis; • Security measures - retention rules; and • Recipients – transfer. • We noted that all of the required information within Article 30 was present within the Force's RoPA. • From reviewing the RoPA we identified within column B the current audit date whilst column F showed the last audit date. We identified a number of blank cells within the last audit date column, but this is due to that data asset only being identified as an asset in 2022. • From the last audit date and the current audit date, we noted that the audit schedule was not specifically completed on an annual basis as originally advised. Further discussion with the GDPR Data Protection Auditor confirmed that all asset owners and guardians have access to the register so that they can update the information where necessary. • The GDPR DPO has advised that going forward the annual audits will be conducted on a rolling basis across the 12 months to allow further work to be carried out in each area and to relieve some of the resource pressure from the auditor. • There is a risk that if the RoPA is not reviewed at least annually, the Force cannot confirm that the information retained is relevant and accurate in line with the GDPR.			
Management Action 1	The Force will ensure that all processing activities are reviewed at least annually to ensure that they are still relevant and up to date and there is clear audit trail of who the auditor has met with and agreed actions.	**Responsible Owner:** Data Protection Auditor	**Date:** 31 October 2023	**Priority:** **Low**

Area: Data Ownership				
Control	Each data asset is assigned an information asset owner who has overall responsibility for the data. Each data asset is also assigned a data guardian within the relevant team, who is responsible for managing the data at an operational level and has more in-depth knowledge of systems and processes. Annual register reviews ensure that information asset owners and data guardians are kept up to date to reflect any changes in staffing.	**Assessment:** **Design** ✓ **Compliance** ×		
Findings / Implications	We reviewed the Information Asset Register which outlines each data asset and the information asset owner. The IMT completes a new data asset record within the register when they are informed of it. If this is not communicated to the team, it will typically be picked up during the annual audit review completed by the GDPR Data Protection Auditor. Asset owners are usually Heads of Department as they take overall responsibility if there is a breach or an issue raised. However, the management of the data on an operational level is a member of the team or department associated with the asset area and they are referred to as data guardians. Asset owners are identified by the individuals directly and report to the IMT. There are currently 17 asset areas not allocated an asset owner within the Information Asset Register. If asset owners or guardian changes are not identified in a timely manner, there is a risk that if a breach occurs there is no individual available to take responsibility and provide a solution.			
Management Action 2	a) Earlier intervention will take place to identify asset owners to ensure they understand their responsibilities. b) Email prompts will be issued to all asset owners on a quarterly basis to identify if owners or guardians have changed.	**Responsible Owner:** Data Protection Officer	**Date:** 31 December 2022	**Priority:** **Medium**

Area: Data Protection Officer resources				
Control	The DPO oversees the IMT and has recently received approval to recruit an additional post within this team for an Information Governance Manager role to support in the fulfilment of the DPO's statutory responsibilities.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	We confirmed with the DPO that she has only been in post since last year and since the development of the role she has completed the ICO self-assessment to identify the gaps within the Force in relation to GDPR As a result the DPO identified a need for additional resources within the team. This was raised by the DPO within the Force Management Statement, that they did not have enough resource available to fulfil the statutory duties. A request was made for an Information Governance Manager role through the force management process. Across the Force over 140 new role applications were submitted and only six were approved due to financial budgets, the Information Governance Manager was one of the roles approved and recruitment is currently underway. Within the IMT, there a Records Manager and a Data Quality Team, an Information Security Manager and an Information Security Team (which includes the GDPR Data Protection Auditor) and an Information Rights Team (comprising of three Information Rights Decision Makers and one Administration Assistant). Records Manager and two Information Management Practitioners. Once the information Governance Manager position is recruited, the team will have sufficient resources to carry out their required tasks, at the moment the team are picking up additional responsibilities to support the function. If the Force is unable to address the priority areas identified by the ICO self-assessment, there is a risk that it may not be able to meet its statutory obligations regarding data protection.			
Management Action 3	Upon appointment of the Information Governance Manager, there should be sufficient priority placed on the outstanding requirements outlined within the ICO Self-Assessment toolkit.	**Responsible Owner:** Data Protection Officer	**Date:** 31 October 2023	**Priority:** **Low**

Area: Individuals Rights				
Control	The Force has an Information Rights Team in place which manage subject access rights across the organisation. In addition, the Records Manager manages any right to rectify and erase. Detailed information is available on the Force's website to ensure that individuals are aware of their rights in respect of data and formal avenues to request Subject Access Requests (SAR) or deletion of data are published. Overall compliance with SARs is regularly monitored across the Force for adequate oversight.	**Assessment:** **Design** ✓ **Compliance** ×		
Findings / Implications	We reviewed the Force's website and confirmed that there is a Data Protection Act 2018 and UK GDPR SAR document published to inform individuals of their rights to request information on themselves or another person for the following: • Disclosures for family court proceedings; • Register sex offenders data (Sarah's Law); and • Domestic violence offender data (Clare's Law). The document clearly outlines how individuals are required to confirm their identity before any information is provided. The website also has a designated section on how to submit a SAR. The page is interactive so that individuals can tailored the options of the dates they are looking to access. Each avenue follows a specific process of how and to whom to submit a request. In discussion with a member of the Information Rights Team, we understood that SARs can be submitted by any means such as; email, post, telephone, in person or via the .gov single online home platform. We also confirmed that the Information Rights Team are required to assess all information requested before disclosing any details to the individual. This is to ensure that there are no breaches for ongoing investigations and it is only the information requested within the agreed parameters. All SARs are acknowledged to confirm receipt and a response is provided within one month of submission. We confirmed with the Information Rights Decision Maker that they currently have no formal procedure document in place to set out the process for SARs and requests for the deletion of data. There is a risk without a procedure document in place, there is no consistency with responses to requestees, and the Force may be unable to set expectations without agreed timescales and decisions.			
Management Action 4	A formal internal procedure will be produced in relation to SARs and the deletion of data to ensure that individuals' expectations are met, and all members of the team are aware of their responsibilities in relation to GDPR.	**Responsible Owner:** Data Protection Officer	**Date:** 30 April 2023	**Priority:** Medium

Area: Consent				
Control	**Partially missing control** The DPO is aware that consent is an area for further development within the Force and has worked with various teams to implement adequate consent processes. However, this is a work in progress and has not been implemented across all Force departments. The DPO completed the ICO's self-assessment toolkit on accountability, which identified areas to work on, including consent arrangements.		**Assessment:** **Design** × **Compliance** -	
Findings / Implications	In discussion with the DPO, we understand that they have already acknowledged that they have further development to undertake in respect of consent. Upon completion of the ICO's self-assessment it is clearly highlighted that the Force requires additional work to be done on consent and this has been a key area for development over the last 12 months. The DPO made the decision to focus solely on one area to identify the needs and requirements before they consider the wider areas within the Force. The DPO made the decision to focus on digital extraction consent as this was a known area which required consent and is one of the areas where consent would be more frequently requested to support investigations. As the DPO has previously implemented a guidance in relation to consent in her prior role, she is hoping to utilise the same guidance within the Force to set out the expectations of when consent is required and what relevant information must be obtained. Within section 6 of the ICO Toolkit it is clear that further development needs to be completed in order to ensure that consent is obtained and managed appropriately. However, we were advised that until the Information Governance Manager is appointed, there is no availability within the team for this level of work to be completed. Within the digital extraction area, the Detective Chief Inspector has developed a digital processing notice which outlines the parameters of the data they require to extract from a device, which is agreed and signed by the individual to ensure that they fully understand the consent they have provided. All digital processing notices are submitted to the Inspector to ensure that the data they have requested is relevant to an investigation and the individual has given appropriate consent. When resource is available, the Force should implement an action plan to outline all data asset areas across each department to ensure there is sufficient focus on consent and ensuring that this is obtained appropriately. Until this is achieved, the Force's ability to meet GDPR requirements in this respect may be undermined.			
Management Action 5	Formal guidance in respect of consent will be produced to help staff and officers support the GDPR requirements in relation to obtaining and the withdrawal of consent. Upon the appointment of the Information Governance Manager, a full review of each asset owner area will be conducted to identify areas where consent is required. Following the area review, a development plan will be created to prioritise areas which require consent.	**Responsible Owner:** Data Protection Officer	**Date:** 30 June 2023 31 October 2023	**Priority:** **High**

Area: Consent		
Control	**Missing control** A Digital Processing Notice Form is available if a device is taken from a suspect or witness.	**Assessment:** **Design** × **Compliance** -
Findings / Implications	As documented in the above control, digital extraction is the only information asset area which has been developed to consider consent. As the digital extraction consent area was developed, the DPO has created three supporting documents to assist in the consent capturing process: • Suspect Digital Processing Notice (DPNc); • Witness Digital Processing Notice (DPNa); and • Witness FAQ Digital Processing Notice B (DPNb). The process for documenting and obtaining consent can vary between witness and suspect. The DNP documents are completed by the on-duty officer alongside the witness or suspect to outline the required information they are looking to extract from the device. The form specifically identified the relevance of the information to be extracted and this is required to be signed and agreed with the witness or suspect directly to give consent. Both witness and suspects forms outline the reason the information or examination of the device is required in order to assist an investigation. Once the form has been agreed with the individual, it is submitted to the Inspector in order to authorise forensic analysis of the device. The authorisation from the Inspector is to ensure that only relevant information is being extracted. For suspects, the process is to request access to the device in question and if they do not comply the officer on duty can instruct seizure of the device in line with the Police and Criminal Evidence Action 1984 section 19. Our findings are limited to the digital extraction area of consent as the process had not been developed and implemented across the wider Force.	
Management Action	*As per management action five.*	

Area: Consent		
Control	**Missing control** Individuals have the right to withdraw consent at any point and can do this via the website, email, or in writing to the DPO / IMT. A member of the IMT will confirm with the individual that their information on record is no longer stored.	**Assessment:** **Design** × **Compliance** -
Findings / Implications	Digital extraction is currently the only area with an implemented consent process. We discussed with the Detective Chief Inspector (DCI) who is the information asset owner in this area, if they had any instances where consent had been withdrawn since the implementation of the device processing notice form. The DCI confirmed that, as there is currently no guidance in place, they do not have a set process to follow, they make judgements on a case by case basis. We were also advised that within the last 12 months, there have only been a handful of instances where an individual has requested that consent be withdrawn. The DCI confirmed that the process was only implemented in August 2022 and they have only had one instance where a victim of sexual assault had requested all information be withdrawn. However, the Deputy Chief Inspector confirmed that at the current stage of investigation into the crime they could not agree to the withdrawal. In this situation, a formal conversation was held with the victim, the DCI and the Crown Prosecution Service to highlight the risks of withdrawing at this stage and if they continued with their consent, they would ensure that only one relevant member of staff associated with the case would be allowed access to the details. Following this discussion, the victim confirmed that she was happy to continue consent on the basis that their information was held in a sensitive manner. For victims or witnesses, withdrawal of consent can disrupt investigations and without a formal procedure in place the investigating officer cannot appropriately advise the individual. Through discussion with the DCI, we confirmed that they currently have no process in place to correctly respond to and advise individuals when withdrawing consent. The DPO confirmed that this was the case and until the Information Governance Manager position is filled, they have no resource to prioritise this.	
Management Action	*As per management action five.*	

APPENDIX A: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Area	Control design not effective*	Non Compliance with controls*	Agreed actions		
			Low	Medium	High
General Data Protection Regulation	1 (13)	4 (13)	2	2	1
Total			**2**	**2**	**1**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

APPENDIX B: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The scope was planned to provide assurance on the controls and mitigations in place relating to the following area:

Objective of the area under review
We will review the Force's approach to compliance with the UK General Data Protection Regulation (UK GDPR), in relation to the use of personal data, and Part 3 of the Data Protection Act 2018 (DPA 2018) in relation to the processing of personal data for preventing, investigating, detecting, and prosecuting crimes. In particular, we will cover the following high-level areas:

1 Business processes and data discovery

Based on the documentation and information provided, review how the Force ensures compliance with the UK GDPR in relation to the use of personal data, and the DPA 2018, Part 3, Section 61 for data being used for law enforcement purposes. Our review will focus on management control processes designed to identify and document all in scope data across the organisation, with particular reference to:

- the existence of processes to map and classify data;
- processes to identify the purpose for the processing of data;
- maintenance of the Register of Processing Activities (RoPA);
- identification and management of data moving from DPA 2018 Part 2 (UK GDPR) into DPA 2018 Part 3; and
- methods of data storage and transfer.

2 Data ownership

Based on the documentation and information at 1 above, note the existence of processes used to identify/allocate data owners.

3 The Role of the Data Protection Officer

Based on the documentation and information provided, review how the Force ensures compliance with the DPA 2018, Sections 69-17 concerning the role of the Data Protection Officer (DPO). In particular:

- whether the Force has a formally appointed DPO;
- whether the DPO is given sufficient priority within the organisation to perform their duties; and
- whether the DPO is afforded sufficient resources to carry out their required tasks.

4 Individual's rights

Based on the documentation and information at 1 above, comment on the existence and operation of procedures in place to ensure compliance with data subject rights across the organisation.

5 Consent

Based on the documentation and information at 1 above, comment on the existence and operation of processes to ensure that the requirements of Article 7 GDPR are complied with in respect of:

- ensuring consent is obtained appropriately;
- documenting when and how consent is obtained; and
- responding when consent is withdrawn.

Limitations to the scope of our work

- The assignment is delivered as an 'agreed upon procedures' review and therefore will not result in a formal assurance level or opinion.
- We will not confirm compliance with UK GDPR or DPA 2018 and/or provide any legal or regulatory advice.
- Our review will not comprise a review of compliance with the Privacy and Electronic Communications Regulations 2013 (PECR).
- Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Debrief held	7 October 2022
Draft report issued	21 October 2022
Revised Draft report issued	31 October 2022
Responses received	1 November 2022
Final report issued	1 November 2022
Revised Final report issued	2 November 2022

Internal audit contacts

Dan Harris, Head of Internal Audit

Philip Church, Senior Manager

Mike Gibson, Client Manager

Hollie Adams, Assistant Manager

Naomi Longstaff, Auditor

Client sponsor

Deputy Chief Constable

Head of Information Management and Data Protection Officer

Distribution

Deputy Chief Constable

Head of Information Management and Data Protection Officer

rsmuk.com