THE CHIEF CONSTABLE OF NORTH YORKSHIRE

General Data Protection Regulation (GDPR) Governance

Internal audit report 12.21/22

FINAL
27 May 2022

1. EXECUTIVE SUMMARY

Why we completed this audit

As part of the approved internal audit plan for 2021 / 2022, we have undertaken a review of the Force's data protection framework and approach to compliance with the UK General Data Protection Regulation (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.

Both the UK GDPR and the supporting Data Protection Act 2018 place an emphasis on organisations, in this case North Yorkshire Police, to implement a framework by which individual's data is held securely, is only used for the purposes specified and data subject rights can be adhered to. As part of this framework, consent is also considered including the methods by which consent is documented and the process by which consent is withdrawn and how this is carried out. The Information Commissioner's Office (ICO) is responsible for regulating data protection and ensuring organisations adhere to the aforementioned laws.

The Force currently has a Data Protection Officer (DPO) and compliance team in place who are responsible for data protection across the Force and ensuring 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 the assets they oversee adhere to GDPR and DPA 2018. Both the information asset owner and the DPO work together on a regular basis though more frequently during the Senior Information Risk Owner (SIRO) assurance process which is undertaken each year. This process alternates each way from a "mini" SIRO statement to a full review. During this process, the asset owner produces either a statement or full review outlining that the processes in place are up-to-date and are accurately recorded on the Information Asset Register (IAR). This is reviewed by the compliance team (including the DPO) and any changes can then be made.

Conclusion

As a result of our review, we have agreed **two high, four medium** and **five low** priority management actions. It should be noted that several of these actions stem from a lack of resources to complete the day-to-day workload and to effectively monitor Force compliance with GDPR and DPA 2018 legislation. The Force has made improvements since a GDPR audit was completed in January 2018, most notably with the hiring of a specialised Data Protection Officer, however there are a number of areas where documentation is not available or is not up-to-date and accurate.

The Force has an IAR which is used as a Record of Processing Activities (RoPA) however we noted that this has not been kept up-to-date and it does not accurately reflect the work that has been completed. We noted that the Force does not have a procedure document outlining the process for transitioning data from Part 2 of the DPA 2018 to Part 3, and vice versa where this applies.

Multiple actions have been agreed relating to training for information asset owners because, whilst training workshops are completed, these are only on a quarterly basis and training records have not been retained. As such, it is not known when asset owners last undertook training related to GDPR, DPA 2018 and other legislation. Furthermore, refresher training is currently not being provided to the information asset owners which presents a risk if changes or updates to data protection legislation are released. A training needs analysis has been completed for both asset owners and the compliance team however the DPO has confirmed that recent guidance published by the ICO means that additional work is required to update the analysis to reflect this.

Procedures have not been established for the right to restrict and the right to object to processing. Whilst the use of these subject rights is uncommon, there is currently no procedure in place to address how this should be processed if an objection was made. A consent register has been created to document how the Force records and documents consent and consent withdrawal however this has not been kept up to date. An audit plan has been created however, apart from several minor tests, this has not been enacted and both consent and compliance with data subject rights has not been tested.

Two resource papers (one for the Police and one for Fire and Rescue) are currently being considered by management to determine whether additional resources are required to help with the day-to-day work within the team. This is especially important as many of these actions and implementation dates are heavily reliant on whether further resourcing can be sourced.

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

Key findings

We identified the following findings that have resulted in two high and five medium priority management actions being agreed:

As part of the various data protection laws, a series of data subject rights have been established which the Force are required to adhere to. As part of these rights, a guidance or procedure document should be in place to provide advice and establish a process by which the Force can respond and comply with these rights. We noted the Force have processes in place for:

- Right to be informed;
- Right to access;
- Right to rectification;
- Right to erasure; and
- Right to restrict processing.

However, we could not locate any reference, process document or guidance for the final three data subject rights:

- Right to data portability;
- Right to object; and
- Rights in relation to automated decision making and profiling.

The DPO confirmed that there is nothing documented for these rights nor are there are any processes in place. There is a risk that if a procedure has not been established and supported by documentation, staff may be unaware on how to deal with a request relating to one of the data subject rights. **(High)**

An audit plan has been created by the DPO to test compliance with GDPR and DPA 2018 legislation. We confirmed that a comprehensive plan has been developed which tests data subject rights and consent however the plan has yet to be fully enacted. The DPO explained that this was partially started when it was first created several years ago however in recent years this has not been fully implemented. As such, the compliance team are limited in the assurance that the Force are adhering to relevant legislation. There is a risk that the Force could be in breach data protection laws. **(High)**

As part of the Data Protection Act 2018, data held by the Force can be held for general processing (Part 2) or for law enforcement processing (Part 3). Data held under the purpose of Part 2 and Part 3 undergoes different processing and has different restrictions. As such, a procedure is needed to clearly identify how and when data is managed when moving from Part 2 (general processing) to Part 3 (law enforcement processing) to ensure the correct restrictions can be applied.

The DPO confirmed that whilst a screening form is in place which is used to identify the transition from Part 2 to Part 3, the Force does not have a policy or procedure document or any guidance for staff to refer to. The DPO explained that this is a national problem and currently no guidance from the ICO has been released and no other force in the region has such a procedure or guidance document. There is a risk that if such a document is not created, staff may be unaware of how to identify and manage such data transitions and could be in breach of data protection legislation. **(Medium)**

Training workshops are held for information asset owners however the dates of when they were attended are not recorded and held. As such, it is not possible to determine when the asset owner last attended training relating to GDPR, DPA 2018 or other data protection legislation. There is a risk that if training records are not held on file, it is not possible to determine whether asset owners require additional refresher training as their original training could be years old. **(Medium)**

Refresher training for information asset owners is currently not being provided. This should be provided to ensure asset owners are aware of any changes to legislation, guidance and to ensure they are more aware of their roles and responsibilities. As such, there is a risk that asset owners may not be up to date on current legislation and guidance and could inadvertently not be complying with legislation. **(Medium)**

The Force has a consent register which is used to document the way different areas process and maintain consent. We reviewed the register and noted there were a number of gaps and fields that were not up to date. For example, one column in the register looks at the withdrawal of consent however, upon review, 37 of the 52 areas are blank or marked unknown. The DPO explained that this is due to a lack of updating and prioritisation of other areas within the Force. Regardless, if the consent register is not fully updated and appropriate review has not been undertaken for the consent process, the Force could struggle to effectively monitor consent and could be in breach of GDPR or DPA 2018 laws. **(Medium)**

For details of the remaining **five 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 confirmed that the information asset register is used to document and identify any asset which uses data. We noted that an assigned asset owner is on file for all and that a description of the asset and purpose for the processing of data is also included on the register. We confirmed that as part of the SIRO assurance process, a statement had been produced in the previous assurance process for 86.2% of assets.

For the remaining 14, a rationale has been provided to explain the delay which has been reviewed by the DPO. For example, six of these statements are with regards to the criminal justice team who have informed the compliance team that due to resource constraints they have not been able to submit a complete statement though the compliance have confirmed that they have been engaging with them.

Data flow diagrams which map and classify data as well as explaining the way they are stored and transferred are required to be completed for all assets that use data. We selected a sample of 20 assets and we were provided with copies of the data flow diagrams for all 20. We noted that there was a range of depth and detail however in all 20 cases a diagram had been completed and was clear how data flowed through the asset.

The Force has a management of electronic storage guidance document and is available to staff to provide guidance on how data should be transferred and stored. We reviewed the reviewed the guidance and verified that several common data storge options were contained within the document (such as the intranet, email, OneDrive) with guidance and advice on how to process and store data within these areas. We noted a responsibilities section at the bottom explaining the roles and responsibilities for all involved in processing or storing data.

A qualified DPO has been appointed by the Force to manage the Force's compliance with GDPR and DPA 2018 legislation. During discussions with the DPO, we confirmed that they were experienced with data security and protection and had worked as a Data Protection Senior Support Officer and Deputy DPO prior to being appointed. In addition, the DPO is working towards the CIPP/E qualification. We confirmed that the Force's website contains the individual's name for the public to view and that the ICO has formally identified this individual as the Force's DPO through a registration certificate.

The DPO confirmed that they felt they had sufficient priority within the Force to complete their responsibilities and held no other role that could disrupt their work.

The Force has several process documents in place regarding data subject rights including:

- Right to be informed;
- Right to access;
- Right to rectification;
- Right to erasure; and
- Right to restrict processing.

These take several forms such as a clear guidance document created specifically for the right (the right to rectification and erasure guidance) or another document in which the right takes only part of the full document (the privacy notice and data protection policy). In all cases we confirmed that the document was up to date, a review cycle had been established and clearly outlined the procedure and advice to staff.

Consent forms are the primary method by which the Force ensures consent is obtained appropriately. Of the 52 areas which require consent, 34 use a consent form. They are reviewed by the DPO and the compliance team to ensure they are appropriate and correctly consider consent. We selected a sample of five areas which have been marked as using a consent form on the Force's consent register and requested a copy of the consent form to determine whether it was clear and appropriately considered consent. In all five cases we were provided with the consent form and verified that this adequately outlined the consent process. For the other areas that do not have consent forms, we noted that consent is recorded via different methods such as the Niche system and that it is the business areas decision on how this is recorded.

A data protection – consent guidance page has been set up on the Force's intranet and is aimed at providing advice and guidance for officers involved in the consent process. We confirmed that officers had access to the page and that this provided a clear introduction to consent.

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: GDPR				
Control	Data flow diagrams are completed for all assets as part of the SIRO assurance statement process by the asset owners. These are reviewed by the compliance team to confirm they are accurate and are in place		**Assessment:** **Design** **Compliance**	 ✓ ×
Findings / Implications	A data-mapping exercise was undertaken in 2019 to identify data and assign responsible and relevant individuals. This has been continued to be used since (though with some changes) to determine appropriate information asset owners. Asset owners are required to create a data flow diagram or map of data detailing how data is used by their asset. Asset owners are expected to review the data diagram on an annual basis as part of the SIRO assurance process to confirm this is up to date. We selected a sample of 20 items from the Information Asset Register and requested copies of the data flow diagrams to confirm these are on file. We verified that a data flow diagram was on file for all 20 assets selected and in all 20 cases we noted that the data flow diagram was clear and included the process of data through the asset as well as the parties involved. Once the diagrams have been initially submitted, they are informally reviewed and quality assured by the compliance team to confirm that they are appropriate, readable and broadly reflect the data used by the asset. As this is an informal review, the results of the review are no typically documented anywhere and we have not been able to provide assurance on whether all diagrams have been reviewed by the compliance team. We reviewed the Information Asset Register and noted that a column has been used to record whether the assets and diagrams have been reviewed however the majority of the fields are empty with the most recent review being 2020. There is a risk that if this column is not kept up to date, it may become unclear on when the data flow diagrams have last been updated.			
Management Action 1	The column in the Information Asset Register relating to whether the assets and dataflow diagrams have been reviewed will be completed.	**Responsible Owner:** Data Protection Officer	**Date:** 31 July 2022	**Priority:** **Low**

Area: GDPR				
Control	The Information Asset Register is used to record all data held and used by the Force as well as the purpose for this data.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	The DPO explained that asset owners are required to input the purpose for the processing of data onto the IAR to ensure the Force are aware of why they hold data. We reviewed a copy of the IAR and confirmed that a dedicated column has been created to input the purpose and that a statement has been included for all 682 rows. We reviewed a selection of these and noted that, whilst there is some repetition on the purpose of processing data, it is clear why data is being processed. The SIRO Assurance Process which is completed each year is used as a review point to determine whether the purpose for the processing of data has changed over the past year. We noted that the IAR has a specific column for the last date of the assurance statement however, upon review, we noted that there were a number of gaps with no dates included or a date from a number of years ago. There is a risk that if the date of the last assurance statement is not recorded or is inaccurate (regardless of whether a statement has been completed since), it may be unclear whether accurate data is stored within the IAR.			
Management Action 2	The IAR will be kept up to date including the date of the last Information Asset Owner Assurance Statement	**Responsible Owner:** Data Protection Officer	**Date:** 31 July 2022	**Priority:** Low

Area: GDPR		
Control	A screening form is used to identify instances when data may be transferred from part 2 to part 3. The form is reviewed by the compliance team to determine whether this accurately contains all information and is correct.	**Assessment:** **Design** ✓ **Compliance** ×
Findings / Implications	There is currently no policy or procedure document in place regarding the changing of data from part 2 to part 3 or vice versa. This is partially due to the lack of national guidance from the ICO and the regional force groups and that no other force in the area or region has a procedure for this (and therefore it has been difficult to benchmark and identify what should be included). Regardless, it was identified by the DPO that this is something that still needs to be implemented and in place. There is a risk that if this document is not created, staff may be unaware of the procedure and the Force could be in breach of data protection legislation. A data impact assessment screening form is used by the Force in instances where functions or processes may have data that moves from Part 2 to Part 3. We reviewed the screening form and discussed this with the DPO who explained that section six and seven within the form look to determine whether data is being transferred from Part 2 to Part 3. The results of these sections are then added to the Information Asset Register. The DPO also noted that there are sometimes one-off instances where functions or processes that do not normally transfer data from Part 2 to Part 3 are required to do so, normally due to court orders. The DPO explained that there is currently no process in place to manage these occurrences but that the procedure document that will be developed will cover this. The DPO explained that each business area is required to hold their own log of any data that has moved from Part 2 to Part 3 including the date and the reason why. Whilst this system is in place, the compliance team and the DPO do not currently check that each team's log is being kept up to date as it is included within the audit plan which is currently not being completed. This has been raised as part of our audit as a high priority action. The screening form is also used by business areas when completing any sort of procurement activities and follows the same procedure for when data moves from Part 2 to Part 3. This involves the business area completing the screening form and sending to the compliance team for the DPO and Deputy DPO to review and determine if it has been completed correctly. As part of this process, the Information Asset Register is updated to outline whether a data protection impact assessment has been considered and required. We reviewed the information asset register and confirmed that all assets are marked as either: • Considered and not required; • Considered and required; and • Not considered.	

	The DPO explained that for those that have been marked as been not considered, this has been due to the team not having sufficient resources to update the Information Asset Register. An action has already been raised as part of this audit to ensure that the Information Asset Register is up to date and we have therefore not raised a new action for this.			
Management Action 3	A procedure document will be created outlining the transition of data from part 2 to part 3 and this will be provided to all relevant staff members (the compliance team, information asset owners). Once national guidance is produced, the produced document will be reviewed and updated to reflect this.	**Responsible Owner:** Data Protection Officer	**Date:** 30 September 2022	**Priority:** **Medium**

Area: GDPR				
Control	Data owners are identified by the compliance team via an update from the Chief Officer Team, the Information Management Lead (who attends the Senior Management Team meeting) or the daily news bulletin.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	As noted previously, a data-mapping exercise was conducted in 2019 to identify data and assign responsible and relevant individuals. Whilst there have been some changes since, for the most part, data assigned to job roles at the time has remained in place. The DPO has informed us that there are multiple ways for the compliance team to identify structural changes where a new data owner may need to be selected. As there are only 23 asset owners and all occupy a senior role within the Force, it is difficult to not identify an asset owner that has moved roles. Monthly updates from the Chief Officer Team are provided which outlines any changes to this team. The Information Lead (who is the DPO's line manager) attends the Senior Management Team meeting in which any changes to the Senior Management Team would be discussed. As most information asset owners are part of the Senior Management Team, any changes would be then brought to the compliance team. An asset owner handbook is provided to new asset owners to provide them with guidance and information on how to perform their role. We were provided with a copy of this handbook and confirmed this contains sufficient guidance and advice regarding the asset owner role. We also noted that the handbook states that asset owners should inform the compliance team if they change their role and are no longer an asset owner. Workshops are held for new asset owners to educate them on their responsibilities and data security and information legislation to ensure the asset owners can correctly complete their job. It was noted that these were held on a quarterly basis as it was not common for asset owners to change however the compliance team are looking to make these more frequent and to expand these to invite "information guardians". Refresher training is also not provided and instead asset owners only receive the training during the initial workshop. If refresher training is not provided to asset owners, they could be unaware of new changes or guidance to data protection (such as from the ICO). The DPO highlighted that whilst training opportunities for data owners has been provided, a record of this has not been retained and the DPO and the compliance team are not aware of when the asset owners last received training. There is a risk that if GDPR training records are not kept for asset owners, they may not receive the required training or refresher training and may not have the appropriate awareness of data security required for a data owner. This could increase the chance of a data breach or an incident where data is not used correctly and could involve an investigation by the ICO.			
Management Action 4	The frequency of training workshops will be evaluated to determine an appropriate frequency. Once this frequency has been agreed, the workshops will be run.	**Responsible Owner:** Data Protection Officer	**Date:** 31 December 2022	**Priority:** **Low**

Management Action 5	Training records for information asset owners will be retained and maintained to ensure all data owners have the appropriate training.	**Responsible Owner:** Data Protection Officer	**Date:** 31 December 2022	**Priority:** **Medium**
Management Action 6	Refresher training will be provided on a set frequency to all asset owners to ensure they are up to date on legislation, their role and responsibilities as a data owner.	**Responsible Owner:** Data Protection Officer	**Date:** 31 December 2022	**Priority:** **Medium**

Area: GDPR				
Control	The DPO leads a team of individuals who are responsible for overseeing GDPR at North Yorkshire Police.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	The DPO leads the compliance team which consists of six members of staff including a permanent Deputy DPO. A further temporary Deputy DPO is currently being recruited. These individuals are primarily responsible for the GDPR and DPA adherence process at North Yorkshire Police. The DPO has explained that the team is currently struggling with workload and does not have sufficient resources to complete their day-to-day work. The DPO noted that as staff are currently completing a heavy workload work is having to be prioritised with low priority work not being completed. Two resource papers have been submitted to the Head of Function and Director to review and, if they agree, the papers will be escalated to the Chief Officer Team. There is a risk that if the DPO does not have sufficient resources, the required tasks may not be fully completed which opens the Force up to potential intervention by the ICO. A training needs analysis has been completed to outline training required for staff within the compliance team and for information asset owners. Whilst this is in place, the DPO noted that this is not up-to-date and needs updating. There is a risk that if the training needs analysis is not complete and up-to-date, key members of staff may not receive the required training and increase the likelihood of non-compliance with relevant legislation. A training report has been provided and from this we can see five of the six compliance team members have completed all training they have been assigned (this includes both training related and not related to data protection and security). For the remaining member, we noted that only one module had not been completed. The DPO explained that the individual has completed the training and this is a recurring technical issue on the system side that has been repeatedly raised however has not been fixed. When reviewing the report, we noted that completion dates were not included. As such, it is difficult for the DPO to determine when training was completed and whether staff need refresher training. There is a risk that if the report is not updated with completion dates, staff may not receive refresher training and may not be fully knowledgeable on the subject of data security and data protection.			
Management Action 7	The training needs analysis spreadsheet will be updated to reflect recent guidance published by the ICO.	**Responsible Owner:** Data Protection Officer	**Date:** 30 June 2022	**Priority:** Low
Management Action 8	Discussions will be undertaken to determine if training dates can be included within the training report.	**Responsible Owner:** Business Insight Lead	**Date:** 30 September 2022	**Priority:** Low

<table>
<tr><th colspan="3">Area: GDPR</th></tr>
<tr><td>Control</td><td>The Force have processes in place outlining the procedures for responding to requests relating to:
Right to be informed;
Right to access;
Right to rectification;
Right to erasure; and
Right to restrict processing.
An audit plan is in place to test officer adherence to these.</td><td>Assessment:
Design ✓
Compliance ×</td></tr>
<tr><td>Findings / Implications</td><td colspan="2">The DPO explained that there are several guidance documents on the Force’s intranet covering data subject rights. The right to be informed is covered within the Force’s privacy notice and data protection policy. We confirmed this was covered and was clear within both documents. We confirmed that a responsibility page was included detailing all individuals involved in the process and their role.

The right to access is covered within the Force’s subject access guidance page and has a detailed section on the background and process for dealing with a subject access application. This is a comprehensive guide and we noted that the final sections relate to monitoring of subject access requests and the dip-sampling noted in the Force’s audit plan. We have raised this as an action during the audit as currently the audit plan is not being enacted however this is covered within a separate control (see management action 12). Subject access requests (SARs) are covered by the Civil Disclosure Unit rather than the compliance team but reporting on subject access requests are provided to the IAB which we have verified.

The Force has a page on the Force’s intranet that covers the right to rectification and right to erasure and provides guidance to staff on upholding this right. We reviewed the page and confirmed this was an in-depth guidance document and contains a responsibilities section for many members of the Force. We also noted that this briefly covers the right to restrict processing though this was not as in-depth as the other rights. Rectification and erasure sits with the compliance team and the DPO and is logged by the team. We were provided with a copy of the log and confirmed that this is being monitored and kept up to date. Upon review of the log we noted that this contains the date when the request was received as well as the person assigned and the resolution of the request. The log goes back to 2018 though we verified that only 147 requests have been received. We confirmed that requests relating to rectification and erasure are reported to the IAB as part of the performance pack each quarter.

The DPO highlighted that the Force do not have procedures for right to restrict processing (GPDR, Article 18), the right to object to processing (GDPR, Article 21) and rights in relation to automated decision making and profiling. It was explained that, whilst there have not been any recorded instances where individuals have objected to processing or asked for processing to be restricted, a procedure does need to be in place for the future. There is a risk that if a procedure is not established and supported by a procedure document, staff may be unaware of how to process or comply with an individual’s request.</td></tr>
</table>

As part of the audit plan, the compliance team test to see whether data and records are adhering to the policies and processes in place for data subject rights. The DPO explained that as part of the plan, compliance staff visit offices and speak to officers to determine whether the policies and processes have been correctly adhered to. For instance, the DPO is scheduled to complete testing several times a quarter to determine whether rectification and erasure decisions have been handled correctly. We have been supplied with a recent example of this review and confirmed this was completed by the DPO.

We have also been supplied with various supporting documents for enacting the audit plan including an information security audit dip sample which looks at both information security and data security. A more targeted information assets dip sample template is available which is designed for assessing assets owned by an information asset owner and tests adherence to GDPR and other data security legislation.

However, whilst the audit plan has been developed, it is currently not fully implemented due to resource constraints. An action has been raised during this review to ensure the audit plan is fully implemented and testing is underway to ensure adherence to the subject access right policies and procedures. There is a risk that if subject rights are not being monitored by the DPO and compliance team, these rights may not be being adhered to and the Force could be failing to comply with GDPR legislation.

The DPO explained that individuals also have numerous options if they wish to raise a concern about how data is being held or used. This includes the data protection inbox which is available on the Force's website, the general enquiries inbox and the ICO who link in with the Force to discuss any complaints or questions.

<table>
<tr><td>Management Action 9</td><td>A procedure will be established for:
Right to data portability;
Right to object; and
Rights in relation to automated decision making and profiling.
Procedure documents will be created to outline these procedures and help guide staff if a request came through.</td><td>Responsible Owner:
Data Protection Officer</td><td>Date:
30 September 2022</td><td>Priority:
High</td></tr>
</table>

Area: GDPR				
Control	A consent register is used by the Force to document the way each consent area documents consent, how it is obtained, where this is located and the withdrawal of consent process.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	Upon review of the consent register, we noted that there were extensive gaps for some of the fields and that the register didn't look fully complete and up to date. We discussed this with the DPO who explained that this is due to staffing issues and the asset owner not getting in touch with the compliance team. For instance, one column in the consent register looks at processes in place for withdrawal of consent. For 37 out of the 52 areas, this is blank or marked as "unknown". As such, it is not possible to determine whether this area has an appropriate process in place for withdrawal of consent and presents a risk to the Force. The DPO explained that the lack of updating this column was partly down to the lack of resources and the prioritisation of other areas over updating the consent register but also the failure of the asset owner to inform the team of this process. Another column within the register relates to whether a consent form has been reviewed by the compliance team. In 11 of the 52 cases, the field has been marked as "No (awaiting copy)" indicating that the asset owner has yet to provide the form to the compliance team. There is a risk that if the consent register is not up to date and appropriate review over consent processes has not been reviewed by the compliance team, the Force could unknowingly be breaching GDPR or data protection legislation through their lack of adequate consent withdrawal processes.			
Management Action 10	The consent register will be fully updated to include up to date information regarding how consent is recorded and stored and to accurately reflect when consent audits were last completed.	**Responsible Owner:** Data Protection Officer	**Date:** 31 March 2023	**Priority:** **Medium**

Area: GDPR				
Control	**Missing control** The compliance team reviews compliance with regards to consent through regular audits.		**Assessment:** **Design** × **Compliance** -	
Findings / Implications	The DPO stated that the compliance team would like to audit the consent process on a consistent basis, especially the withdrawal of consent, to ensure that officers are complying with GDPR and other legislation. However, given the current workload and due to the Covid-19 pandemic, this has not been possible on a consistent basis. An audit plan has been developed and, upon review, it is clear that work has been undertaken to develop a schedule of audits to be completed (including dip sampling) but this has not been completed on a regular basis. Within the consent register is a column which outlines the date of the last consent audit. We noted that for many of these areas, the audit column is blank or an audit was completed a number of years ago. We also noted that the audit plan contains scheduled audits for other areas such as compliance with rectify and erase procedures but they are in the same position as the consent audits. There is a risk that if the audit plan is not enacted, the Force could be in breach of data protection legislation which could negatively impact the Force's reputation and see the issuing of fines.			
Management Action 11	The audit plan will be enacted by the compliance team to ensure monitoring of the Force's compliance with GDPR, DPA and other legislation.	**Responsible Owner:** Data Protection Officer	**Date:** 30 September 2023	**Priority:** **High**

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 management actions		
					Low	Medium	High
GDPR	1	(13)	8	(13)**	5	4	2
Total					**5**	**4**	**2**

* 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.

** More than one management action has been raised against a given control.

APPENDIX B: SCOPE

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

This document sets out the key information relating to the internal audit assignment, including the dates and agreed deadlines, the assignment team and client staff to be involved, and most importantly the scope of the assignment, including the limitations to the scope.

Scope of the 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	6 April 2022
Additional evidence received	22 April 2022
Draft report issued	3 May 2022
Revised Draft report issued	19 May 2022
Responses received	27 May 2022
Final report issued	27 May 2022

Internal audit Contacts	Dan Harris, Head of Internal Audit Philip Church, Senior Manager Mike Gibson, Client Manager Oliver Gascoigne, Lead Auditor
Client sponsor	Managing Director Head of Business Design and Assurance Management Information Lead Data Protection Officer
Distribution	Managing Director Head of Business Design and Assurance Management Information Lead Data Protection Officer