THE POLICE AND CRIME COMMISSIONER FOR NORTH YORKSHIRE AND THE CHIEF CONSTABLE OF NORTH YORKSHIRE

General Data Protection Regulation (GDPR) Governance

FINAL

Internal Audit Report: 8.17/18

16 February 2018

RSM

CONTENTS

1 Executive summary 2
2 Detailed findings 7
Appendix A: Scope 23
Appendix B: Further information 26
For further information contact 27

Debrief held	12 January 2018	**Internal audit team**	Dan Harris, Head of Internal Audit
Draft report issued	25 January 2018		Angela Ward, Senior Manager
Responses received	16 February 2018		Philip Church, Client Manager
			Eddie Ndhlovu, Senior Auditor
Final report issued	16 February 2018	**Client sponsor**	Interim Chief Executive Officer
			Deputy Chief Constable
			Force Solicitor and Head of Legal Services
		Distribution	Interim Chief Executive Officer
			Deputy Chief Constable
			Force Solicitor and Head of Legal Services

1 EXECUTIVE SUMMARY

1.1 Background

The General Data Protection Regulation (GDPR), including the Data Protection Bill (the Bill), will be implemented on 25th May 2018. The GDPR will replace European Union (EU) Directive 95 / 46 / EC on which the UK Data Protection Act is based with a single EU-wide regulation. It is likely to remain after the UK leaves the European Union. It is also extremely likely that any post-Brexit UK privacy legislation will retain significant elements of the GDPR. As a result, the Information Commissioner's Office (ICO) has recommended that it is now essential for organisations to start planning their approach to formal GDPR compliance.

GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. With that in mind, the ICO has published a 12 step guide setting out how organisations can begin their preparations for the changes.

Many of the GDPR's main concepts and principles are largely the same as those in the current Data Protection Act so much of the current approach to compliance will remain the same. However, there are significant new elements and enhancements which will require the Police and Crime Commissioner (PCC) for North Yorkshire Police (NYP) and the Chief Constable of North Yorkshire (the Force) to perform some specific compliance activities for the first time.

In April 2016, the EU agreed the Law Enforcement Directive ("LED") to govern "the processing of personal data by the police and other criminal justice agencies for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data". The LED applies in relation to the cross-border processing of personal data for law enforcement purpose. To ensure a coherent regime, the provisions in the Bill also apply to the domestic processing of personal data for such purposes. This seeks to ensure that there is a single domestic and trans-national regime for the processing of personal data for law enforcement purposes across the whole of the law enforcement sector.

The PCC and the Force have a joint Legal Services Team which is currently overseeing the process of ensuring both organisations are compliant with the GDPR requirements by 25th May 2018 which is led by the Force Solicitor and Head of Legal Services and Police Lawyer - Civil Disclosure Unit (CDU). A joint working group was set up with management representatives from the Force and the office of the PCC. At the time of the audit, two meetings had been held in October and November 2017. As roles and responsibilities have been assigned, further work has been completed since the November meeting. In addition since November and the time of our audit a briefing has been provided to the senior management team.

The Force has set aside £50,000 inclusive of on-costs (£35,000 excluding on-costs) for the recruitment and appointment of a Data Protection Officer (DPO). At the time of the audit, the recruitment of the DPO was yet to be undertaken although authorisation to recruit had been sought from the Force's Chief Finance Officer. The PCC's Chief Finance Officer has set aside an allocation for both the Force's and PCC's Data Protection Officers in the Medium Term Financial Plan.

The PCC submitted a local business case to the Home Secretary in October 2017 in which to transfer the governance of North Yorkshire Fire and Rescue Service (NYFRS), from the current North Yorkshire Fire and Rescue Authority to a Police, Fire and Crime Commissioner. At the time of the audit, no decision had been made by the Home Secretary to decide in favor of the business case. As yet, no firm decision had been made in appointing a permanent DPO for the PCC, however it was envisaged that a current member of staff would assume DPO responsibilities on an interim basis.

1.2 Conclusion

Whilst the Force / PCC have undertaken a GDPR readiness gap analysis, established a GDPR Working Group and identified information asset owners to complete the data mapping exercise. The data mapping exercise is a key component in understanding what personal information is collected and processed by the organisations.

Priority should be given to the completion of the data mapping exercise and produce an action plan to ensure GDPR compliance is achieved, consent audit and the appointment of DPOs. The Force has assigned a project manager (three days a week) to manage the GDPR agenda and business analyst (one and half days a week) to assist with the data mapping exercise. The Data Protection Officer (DPO) at the Force is scheduled to be advertised week commencing 12th February 2018.

1.3 Key finding

The key findings from this review are as follows:

Business processes and data discovery

- We noted that both organisations are in the process of planning to undertake data-mapping exercises in order to identify what data exists across the organisations; how the data is used; and how the data is shared and ultimately to create an all-encompassing fit-for-purpose Information Asset Register (IAR). However, we identified a GDPR readiness action plan was not in place to ensure that the data mapping exercise will be completed in a timely manner.

- A gap analysis had been undertaken by both the Force and the PCC to assess the “as-is” position, the result of this has been documented. However, a GDPR readiness action plan was not in place to ensure all activities identified are undertaken in a timely manner.

  For note: The Force should be aware that this process could take several months (since there are over 240 information systems, and other applicable data probably flows aside from these assets).

Third parties

- The organisations have various information sharing agreements in place with key partners and authorities. The details of third party sharing agreements are held in an information sharing register. However, there was lacking a data flow mapping exercise detailing the flow of data to various places, including third parties.

  We also noted that both organisations did not have a documented plan designed to ensure that the contracts in place with third parties had been updated to include details on GDPR. The Force has assigned a project manager and business analyst some time to assist in the preparation work for the data mapping exercise.

Data ownership

- There is an Information Asset Owner (IAO) Handbook in place for the Force which details the role and responsibility of IAOs. The Information Security Officer has scheduled interviews with identified IAOs. However, the organisations have not finalised its information assets in its information asset register.

- The Information Security Officer confirmed IAOs would be identified as part of the data mapping exercise. Meetings between the Information Security Officer and IAOs had been scheduled at the time of the audit.

Data security system controls

- Discussions with the Chief Digital Information Officer confirmed the organisations have planned to implement an Information Security Management System (ISMS). An ISMS is a system of processes, documents and technology that helps to protect information through a centrally managed framework.

- Most of the systems (over 240) are currently managed in silos with no current oversight to ensure the password policies are applied in line with best practice. However, at the time of the audit, there was no documented plan in place detailing the activities to be undertaken to ensure all systems are managed through a central framework to ensure compliance with the GDPR.

Data storage and retention

- There is a Records Management Policy in place, together with a data retention and storage procedure schedule, setting out the guidelines for the retention of information and data across the Force. However, this will soon be out of date and will need to be reviewed to reflect GDPR requirements.

- The planned data mapping exercise will identify all systems and storage in order to document where each asset is stored. The PCC does not have as many systems in place, therefore the exercise should be less time consuming.

Awareness

- There is general awareness of the GDPR is promoted through team meetings, the Information Assurance Board and senior management briefings and via the intranet. In addition, the GDPR Working Group has representatives from various departments, including staff from the Office of the Police and Crime Commissioner (OPCC).

- Discussions with the Police Lawyer (CDU) established that the organisations are waiting for the national training module to be rolled out for all staff to complete. No date has been announced for this to be rolled out, however it is envisaged that it will be before the May implementation date.

- We noted that the organisations are yet to produce a communication strategy to raise awareness of GDPR requirements.

Data policy, roles and responsibilities

- The Data Protection Policy and other associated data protection policies will soon be out of date and the information contained within them superseded by the introduction of the GDPR. There is currently no plan, with implementation dates in place, for addressing the need to review all related policies to ensure they reflect the GDPR requirements. The requirement to review key policies and procedures has been highlighted as part of the gap analysis undertaken by the organisations.

- Review of the proposed role of Data Protection Officer at the Force identified that it was not in line with recommendations made in the paper entitled 'The Role and Position of the Data Protection Officer within the Police Service.' The following areas were not currently reflected by the Force:

  - The requirement to appoint a DPO at an appropriately senior level such as Head of Information Management. The Force's proposed DPO is not at this level and will report to the Police Lawyer within CDU;

  - Consideration given to the role of DPO as being best aligned to the Head of Information Management/ Information Governance Manager role if it is not already, as both the Records Management and Information Security Assurance functions will be required to report to the DPO for that person to fulfil their tasks;

  - Although discussions had been held with the Chief Finance Officer and the Head of HR in relation to providing extra resources for the DPO to fulfil the role and exercise their statutory tasks, this was yet to be agreed. It is envisaged that with the perceived demand, the subject access rights may cause forces to have additional resources in order to process requests; and

  - Requirement to provide arrangements for business continuity by the DPO by having in place a deputy data protection officer.

- The Police and Crime Commissioner (PCC) is considering the appointment of a current staff member on an interim basis pending the decision from the Home Secretary about the submitted business case for the proposed transfer of governance of the NYFRS. However, the DPO's job description had not yet been reviewed at the time of the audit. Subsequently, the position of DPO was advertised on 12th February 2018.

Individuals' rights

- We were informed that the existing privacy notices relating to data subject's individual rights will be updated in line with GDPR and Data Protection Bill requirements. However, a documented plan with responsible owners and dates for completion was not in place.

  The privacy notices will need to contain all the individual rights as required by the GDPR and published for all data subjects to be aware of their enhanced rights under the GDPR.

Consent

- We noted that as part of the gap analysis undertaken, the organisations have identified the need to review its consent processes via the data flow mapping exercise scheduled with the information asset owners. However, at the time of the audit. There was no documented plan, with implementation dates, in place to ensure this was completed in a timely manner.

- The organisations have not undertaken an exercise, through a consent audit, to identify whether explicit consent had previously been obtained, or whether retrospective consent is required.

- We noted that there is no process in place or documented plan for reviewing and refreshing children's consent at appropriate milestones, as per the ICO guidelines.

Data breaches

- Review of the Security Incident Reporting Procedure confirmed that it sets out the steps to detect, respond and recover from an incident, including a personal data breach. Furthermore, following a recent data breach reported to the ICO, it was noted that the organisations processes for investigating breaches in place, reporting to the ICO and notifying the data subjects affected. It was also noted that there were processes in place to ensure that there is an audit trail for inappropriate access to the organisations' systems.

- The gap analysis identified the Security Incident Reporting Procedure had not been updated to reflect the following:

    - Include in the procedures the data protection officer to whom data breach will be reported;

    - Include in the procedures the types of data breaches as defined by the ICO;

    - Include procedures for reporting data breaches by third parties;

    - Have mechanisms in place to ensure the organisation will report data breaches to the ICO within 72 hours where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach; and

    - Inclusion of the rule that failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Law Enforcement Directive (LED) / Data Protection Bill

The gap analysis undertaken identified the impact of the LED however a formal plan had not been developed to address the following areas:

- Classification / identification of different categories of data subjects (such as victims, witnesses, offenders);

- Classification of whether the data is fact or personal opinion/assessment; e.g. witness statements vs. factual evidence;

- Although it was identified that there were some systems, such as niche, which provided an audit trail and logs of access. There were outstanding exercises to be undertaken of the functionality of all automated systems to ensure that the Force is able to keep logs of processing operations in automated processing systems. This should include a log of any alterations to records, access to records, erasure and disclosures of records unless an exemption applies;

- Review of procedures for transferring or sharing personal data across borders (either with relevant authorities or others) to ensure that they are compliant; and

- Ensuring there is an appropriate policy in place for the sensitive processing of data with the extra inclusion categories of sensitive processing of data including genetic or biometric data which would also need to be included.

2 DETAILED FINDINGS

Our internal audit findings and the resulting actions are shown below.

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
1	Business processes and data discovery	The main focus of the GDPR is protecting the digital rights of individuals who are referred to as data subjects. All personal data collected from data subjects should be audited and documented to ascertain what is being held and for what purpose. The Force and PCC are currently planning audits to identify what data exists across each department, how it is used and shared. Informal exercises have also begun in a number of departments. At the time of the audit, the organisations have completed a gap analysis of the 'as-is' process with a view of completing a data mapping and flow exercise. We identified that the organisations have an information asset register in place but this is two years out of date and not fit for purpose i.e. it did not include the following information: • The location and origin of all personal data held in-house; • How the data is stored; • The classification of each piece of personal data; • Whether arrangements are in place for the data to be shared internally or with a third party; and • A clear data owner assigned against each piece of data. Discussions with the Information Security Officer confirmed that there are plans in place to undertake a data audit. We noted that calendar dates had been set with various individuals who had been identified as potential data asset owners. Furthermore, we noted that information to be sought from data owners was documented and upon review contained information required by the GDPR, such as classification of	The organisations will document an action plan in relation to the GDPR which will include gap analysis headings and the following key items: • Actions to be undertaken; • Responsibility; • Timeframes; • Progress indicators; and • Monitoring activities to be undertaken. A record will be maintained of: • The location and origin of all personal data held in-house; • How the data is stored; • The classification of each piece of personal data; • Whether arrangements are in place for it to be shared	Police Lawyer (CDU) Information Security Officer Head of Information Management	25th May 2018

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		data handled by the Force. A gap analysis was undertaken by both the Force and the PCC to assess the "as-is" position, the result of this has been documented however to date there is no action plan in place to address the outcome of the exercise. Undertaking a data discovery of all information assets and data systems would enable the Force to carry out a risk assessment in order to put in place appropriate mitigating actions against the identified risks. Documenting the plan, along with the associated dates of completion and staff responsible, would ensure accountability and effective monitoring of the data mapping / discovery plan. With only four months left until the compliance date of 25th May 2018, there is a risk that the organisations may not be in a position to complete the data flow mapping exercises on time. Examples of potential non-compliance include: • The inability to notify third parties of any inaccuracies in data shared with them, due to lack of awareness of the information sharing arrangements in question; and • Non-compliance with the GDPR accountability principle by demonstrating that the organisation has effective policies and procedures in place for the management of personal data.	internally or with a third party; and • A clear data owner assigned against each piece of data. Once completed, a process will be implemented to ensure that this central record, resulting from the data audit, is accurate and remains up to date to ensure that the organisations continue to hold a comprehensive record of all the personal data held. This could be assured by regular data audits to capture any changes.		

Risk Exposure			Root causes		
Non-compliance with the GDPR.			Lack of formal plans to address the gap analysis undertaken.		
Probability	**Financial**	**Reputational**	**Operational**	**Legal**	**Rating**
Probable	Severe	Severe	Significant	Severe	2:15

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
2	Third parties	As the data audit / data mapping exercise had not yet been undertaken by the organisations, there was not an accurate record of the location and origin of all personal data held in-house or shared with third parties. We noted that there was a process in place for capturing information sharing agreements with third parties, however this was not linked to the information asset register but this was identified as part of the gap analysis performed. Having an accurate and up-to-date information asset register would enable the organisations to be aware of the third parties data is shared with as well as knowledge of whether or not an information sharing agreements have been put in place, agreed and signed. Review of a pro-forma information sharing agreement identified that it would soon be out of date and would therefore need to reflect the GDPR requirements. We determined that data and information sharing agreements are included in contracts with third parties. However, it is likely that the contracts will need to be updated with the advent of the GDPR to reduce the likelihood of non-compliance with the regulation. The PCC and the Chief Constable are both data controllers and data processor under data protection laws. Both share information with each other and also share information with other third parties. As the GDPR demands increased accountability from the data controller for data processing, there is a greater responsibility for ensuring that organisations know what information is shared with third parties to reduce the risk of non-compliance with GDPR and potential fines. The GDPR places data processors under a direct obligation to comply with certain data protection requirements which previously only applied to data controllers. These obligations mean that data processors may be subject to direct enforcement by supervisory authorities, serious	The PCC and the Force will undertake the following: • Ensure that all data sharing agreements with third parties are GDPR compliant; • Ensure a data flow mapping exercise is undertaken for every third party; • Ensure that third party contracts are updated so that the data sharing and confidentiality agreements reflect the standards set by the GDPR; and • Where necessary, undertake retrospective GDPR due diligence exercises to ensure third parties can demonstrate adequate processes are in place for compliance.	Police Lawyer (CDU)	25th May 2018

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		fines for non-compliance and compensation claims by data subjects for any damage caused by breaching the GDPR. This therefore, means that in order to be both organisations may need to undertake retrospective GDPR due diligence exercises to ensure all third parties the organisations share data with have satisfactory processes in place.			
3	Data ownership	Discussions with the Information Security Officer noted that data owners had been identified and meetings were to be held in order to complete a data mapping exercise. It was envisaged that the identified data owners would be documented in the information asset register. Furthermore, training was scheduled with the data owners to ensure they were aware of their roles and responsibilities in this regard. A formalised plan to meet with the 20 identified data owners had not been documented to ensure the exercise was effectively monitored and any slippages reported to the GDPR Working Group.	The organisations will formalise their arrangements for the completion of the mapping exercise to ensure that all data and data owners have been captured. Once the data flows have been mapped, a review of the data owners will be undertaken to ensure those identified are still appropriate.	Police Lawyer (CDU) Information Security Officer Head of Information Management	25th May 2018
4	Data security system level controls	There is an Information Security Policy in place detailing the security of assets and how access is controlled to systems and any other information assets. We noted through discussion with the Chief Digital Information Officer that access to systems (over 240) across the Force was delegated to asset owners as detailed in the current register. Therefore, most of the systems were currently managed in silos with no current oversight to ensure the password policies applied are in line with best practice. The Police and Crime Commissioner is (PCC) office did not have many systems in place. It was however, noted that the main Windows logon password policy was in line with good practice i.e. password protected and must contain eight characters or greater and a mix of: • At least one uppercase character; • At least one lowercase character;	The organisations will put in place a formalised plan to ensure access controls to the systems are appropriate and associated password policies are managed centrally in line with best practice. In the long term, the organisations will look at the implementation of ISMS system in order to help protect information in line with the GDPR.	Chief Digital Information Officer	25th May 2018

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		• At least one number; and • Cannot use passwords similar to previous ones. The GDPR requires organisations to take necessary technical and organisational measures to ensure a high level of information security according to Article 32: security of processing data. Although examples of security measures and controls are cited, the GDPR does not provide detailed guidance on how to achieve this. We noted that the organisations have achieved ISO 27001 accreditation which is an international standard for information security. Discussions with the Chief Digital Information Officer noted that the organisations were planning to implement an Information Security Management System (ISMS).			
5	Data storage and retention	There is a record of all information assets documented on the intranet, however this is currently two years out of date. The organisations have undertaken significant work to update this information. We noted that there were over 240 systems in place across both organisations. There are plans for identifying systems and applications used to retain and store data, the data will be identified as part of the audit. There is a Records Management Policy in place, as well as data retention and storage procedure, detailing the retention of data across the organisations. However, these would soon be out of date and would need to be reviewed ahead of the GDPR. Discussions with the Records Manager confirmed that records retention and management audits were currently not undertaken by a central team. We noted that this was a head of department responsibility and currently there was a lack of compliance audits carried out to ensure information is retained and archived accordingly. We noted that the disposal and retention for both paper and electronic	The organisations will undertake the following: • Put a plan in place to review associated policies for storage and disposal of data; • Produce a comprehensive, accurate and up to date record of all data storage and retention locations, including back-ups. This will be supported by relevant policies and procedures; and • Put in place a plan to ensure that audits are carried out in accordance with data retention	Head of Information Management	25th May 2018

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		data were yet to be documented to ensure data was not stored beyond the retention schedule dates. Through discussions with the Head of Information Management we confirmed that there were currently national plans in place with one of the main customer relationship management systems, Niche, to automate the process of deleting data stored within the systems. This would ensure compliance with the Management of Police Information (MoPI) Code of Practice retention rules. However, at the time of the audit, the process of deleting data was manually undertaken by the Records and Information Management team and there were no audits carried out to ensure that the MoPI Code of Practice was being adhered to. To ensure compliance with the retention and disposal schedule, the Force should look to produce an automated process on their related systems. This would further strengthen the tracking, tracing and monitoring of records. We also confirmed that as part of the GDPR gap analysis, the organisations have identified a framework to allow the identification of instances where a Privacy Impact Assessment (PIA) would be required. However, at the time of the audit, the process of having PIAs at the start of projects or initiatives involving the processing of personal data was yet to be assigned an implementation date and a specific plan for this was not yet documented. Without a process and framework for conducting PIAs, there is an increased risk that the organisations will fail to comply with GDPR requirements regarding Data Protection by Design and Data Protection PIAs.	policy / procedure and MoPI Code of Practice. The organisations will ensure that their data protection by design and privacy impact assessment processes are reviewed. This should include the following: • The now express legal requirement for organisations to take a 'privacy by design' and data minimisation approach; and • PIAs are required for high-risk situations, for example where a new technology is being deployed or where a profiling operation is likely to significantly affect individuals. If the PIA indicates high-risk processing, e.g. new technology, the ICO will need to be consulted.	Police Lawyer (CDU)	25th May 2018
6	Awareness	**Management** A GDPR Working Group is in place with representatives from various departments including:	The organisations will undertake the following: • Ensure there is a communication strategy in place with detailed timescales	Police Lawyer (CDU)	25th May 2018

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		• The Police Lawyer (Civil Disclosure Unit); • Information Security Officer / Head of Information Management; • Finance Manager; • Governance and Delivery Manager; • Change Analyst; • Procurement; • Force Solicitor and Head of Legal Services; • OPCC; • Human Resources Manager; • Head of Corporate Communications; • Head of Risk and Assurance; • Chief Digital Information Officer; • Operational Development; • Training lead; and • Head of Estates. Meetings were scheduled to be held on a monthly basis. We noted that since the formation of the group, two meetings had been held in October and November 2017. The group was yet to produce a comprehensive action plan, with action owners and implementation	for updates on the GDPR leading up to and beyond the implementation date of 25th May 2018; • Once officially appointed, the role of the DPO will be communicated to all staff; and • Pending the release of a national training programme for GDPR, ensure there is a plan in place to check all staff have completed the training before 25th May 2018.		

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		dates, to address all the GDPR requirements and ensure compliance by 25th May 2018. **General staff** Discussions with the Police Lawyer (CDU) established that the organisations were waiting for the national training module to be rolled out for all staff to complete. At the time of the audit, data protection training provided by the National Centre for Applied Learning Technologies (NCALT), a collaboration between the College of Policing and the Metropolitan Police Service was at 40 per cent. It should be noted that the NCALT training was made mandatory in August 2017. It would be prudent to complete the training as early as possible to ensure that there is sufficient time available to ensure that all staff are sufficiently trained and aware of GDPR requirements. Review of the GDPR communication sent out in January 2018 noted that it did not sufficiently address what GDPR was and the key themes / changes that staff should be aware of. We noted that the organisations were yet to produce a communication strategy to ensure that the organisations' major decision makers and managers and all other employees are fully aware of the forthcoming GDPR legislation. This will also need to include detail of the DPO and how staff can access them.			
7	Data policy, roles and responsibilities	**Policies and procedures** The Data Protection Policy and other associated data protection policies will be out of date and the information contained within them will be superseded by the introduction of the GDPR. This had been identified as part of the gap analysis but no formal plans were to address this. **Roles and responsibilities**	The organisations document their plan to review and update the Data Protection Policy and other associated policies in line with GDPR requirements and ensure these are communicated with all relevant staff prior to 25th May 2018. Furthermore, the Force will undertake the following:	Police Lawyer (CDU) Force Solicitor and Head of Legal Services Head of Information Management	25th May 2018

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		The GDPR has made it mandatory for the Force and Police and Crime Commissioner (PCC) to appoint a designated data protection officer. Although there are no specific qualification requirements within the EU data protection officer guidelines, there is mention that the data protection officer shall be designated on the basis of professional qualities and have expert knowledge of data protection law and practices and the ability to fulfil his or her tasks. At the time of the audit, roles and responsibilities for the area had been defined and recruitment was currently being undertaken for the position of a DPO within the Force. Review of the proposed role of DPO at the Force identified that it was not in line with recommendations made by the National Police GDPR Working Group paper 'The Role and Position of the Data Protection Officer within the Police Service.' The following areas were not currently reflected by the Force: • The requirement to appoint a DPO at an appropriately senior level such as Head of Information Management. The Force's proposed DPO is not at this level and will report to the Police Lawyer within CDU; • Consideration given to the role of DPO as being best aligned to the Head of Information Management / Information Governance Manager role if it is not already, as both the Records Management and Information Security Assurance functions will be required to report to the DPO in order for the DPO to fulfil their tasks; • Although discussions had been held with the Chief Finance Officer and the Head of HR in relation to providing extra resources for the DPO to fulfil the role and to exercise their statutory tasks, this was yet to be agreed. It is envisaged that with the perceived demand, the subject access rights may cause forces to need additional resources in order to process requests; and	• Ensure that a DPO is in post prior to 25th May 2018; • Appoint a DPO at an appropriate level with high level of expertise and skills; • Consider the recommendations made in 'The Role and Position of the Data Protection Officer within the Police Service' paper; • The need for roles with data protection responsibilities is identified within their structure and governance arrangements; • Ensure that the roles are formally allocated to individuals with the knowledge, support and authority to carry out the duties associated with GDPR effectively; • Identify and formally put in place additional roles which will provide support to the GDPR activities; • Ensure that relevant individuals receive appropriate training to undertake their roles effectively; and • Ensure the data protection officer has sufficient resources		

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		• Requirement to provide arrangements for business continuity for the DPO by having in place a deputy data protection officer. The Force has set aside £50,000 inclusive of on-costs or £35,000 excluding on-costs for the recruitment and appointment of a Data Protection Officer (DPO). At the time of the audit, the recruitment of the DPO had not been undertaken however authorisation to recruit had been obtained from the Force's Chief Finance Officer. It was noted that the Force and the Police and Crime Commissioner (PCC) would not be sharing a data protection officer. The PCC was considering the appointment of a current staff member, on an interim basis, who reports to the Interim Chief Executive Officer. Furthermore, there was a reluctance to appoint a permanent DPO due to the outstanding business case yet to be approved by the Home Secretary in which there is a proposal of a transfer of governance of NYFRS.	both time and financial to carry out their duties which will include regular compliance audits.		
8	Individuals' rights	We noted through discussions with the Information Security Officer that work was due to commence with identified information asset owners to capture privacy notice information which would be done as part during the data mapping exercise. The GDPR provides the following rights for individuals: • The right to be informed; • The right of access; • The right to rectification; • The right to erasure; • The right to restrict processing; • The right to data portability; • The right to object; and	The organisations will put comprehensive plans in place with responsible owners and timescales to ensure that individual rights processes are in place. The organisations will ensure there is clear, concise, easy to understand privacy notices which are accessible to all data subjects in particular victims, witnesses, suspects and staff via the organisations' website, intranet or leaflets to provide information on the following: • What information is collected by organisations from individuals; • What the records are used for;	Police Lawyer (CDU)	25th May 2018

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		• Rights in relation to automated decision making and profiling. We noted that there was a "How We Use Your Information" document which explains how North Yorkshire Police obtains, holds, uses and discloses information about people (personal information), the steps they take to ensure that it is protected, and also the rights individuals have in regard to their personal information handled by North Yorkshire Police. Consideration should be given to have in place a number of privacy notices which covers information related to all data subjects, ensuring that these are in an easily accessible form and are ready by May 2018. The organisations will need to include more detailed information including the lawful basis for processing personal data and retention periods unless an exemption applies. **Subject access requests** To process subject access requests, the Force currently had 40 days to undertake and a £10 processing fee was applicable. Under GDPR, subject access requests should be free of charge and the time taken to process the requests will be reduced to 30 days. Due to the requirement to publish the rights of individuals under GDPR there is a perceived increase in demand in relation to subject access requests. This would therefore require more resources to comply with the timeframes. Currently the Force was operating at 60 per cent compliance. The processing of rights of individuals, such as rights to erasure, was currently done manually by staff within the CDU department. This was very time consuming and there was no guarantee that all information in relation to a specific data subject would be deleted from all the systems. With over 200 systems in place and a lack of an automated process, the task of deleting data would become onerous. In order to cope with demand, the organisations will look into having all of its data in electronic format and have systems linked with each other to ensure the process of dealing with individual rights is automated at each point.	• How the records are kept confidential; • The partnership organisations with whom information may be shared; • Rights for individuals to view their records; • Legal basis for processing data; • Data retention periods; • Right to complain to the ICO; • Detailed procedures for how to withdraw access to their personal information; and • Detailed GDPR individual rights. The organisations will also review and consider the automation of the process of the systems used to ensure that data subject information can be deleted / rectified efficiently if requested by data subjects. The organisations will also amend all staff contracts to include updated information for compliance with GDPR.		

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		This would increase the organisation's confidence in dealing with data subject rights. Discussions with the Chief Digital Information Officer noted that the organisations are currently not in a position to automate all of their processes and data in such a way that rights of individuals could be processed in an efficient and effective manner.	The organisations will update any related policies for subject access requests under GDPR which will include: • The right to have information provided in a commonly used and machine-readable format; • A 30-day limit on transmission of information; and • The right to have a free provision of access to their information.		
9	Consent	**Consent – seeking consent** We noted that as part of the gap analysis undertaken, the organisations were going to review their consent processes via the data flow mapping exercise. However, as at the time of the audit, there was no documented plan in place for the organisations to review processes in place for seeking, obtaining and recording consent. Furthermore, various departments were yet to be contacted as part of the consent audit to ensure that all consent documentation was in line with the GDPR requirements. Processes for seeking, obtaining and recording consent to handling individuals' personal data should be identified and documented in a comprehensive action plan. Once all methods are identified, they should be reviewed and updated in accordance with the requirements of the GDPR. The requirements for consent processes under the GDPR include:	The organisations will ensure that: • Processes for seeking, obtaining and recording consent to handling individuals' personal data are identified; • Once all methods are identified, they will be reviewed and updated in accordance with the requirements of the GDPR; • Review systems for recording consent to ensure there is an effective audit trail and to demonstrate consent has been given; • Undertake consent audits;	Police Lawyer (CDU)	25th May 2018

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		• Explicit consent must be given for data collection, data usage and marketing; • Consent must be verifiable / subject to an appropriate audit trail; and • There must be positive indication of agreement of personal data being processed i.e. this must not be inferred from silence, pre-ticked boxes or inactivity. The organisations have not yet undertaken an exercise whereby, where it relied on consent, consideration had been given as to whether this was appropriate or if it should use another lawful basis. If consent is appropriate then they should review how they seek, record and manage consent and whether you need to make any changes. The organisations would need to refresh existing consents if they do not meet the standard required. Consent audit exercise should be reviewed for the following data subjects and areas: • Victims; • Witnesses; • Suspects; • Current members of staff; • Marketing; • Communications; • Website usage;	• Review all previous methods of obtaining consent on data held to identify whether explicit consent was received. If not, retrospective explicit consent will be sought; • Implement a process where there is review and refresh of children's consent at appropriate milestones; and • Management will consider developing their IT systems to enable efficient 'SAR' and 'Forget Me' processes.		

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		• Applicants at the recruitment stage; and • Applications for the cadets etc. **Consent – retrospective** The organisations have not undertaken an exercise to identify whether explicit consent has previously been obtained, therefore if retrospective consent is required. The organisations cannot identify where they will need to obtain retrospective consent and this may result in a breach of the new GDPR rules. **Consent – children** We confirmed there was no process for reviewing and refreshing children's consent at appropriate milestones, as per the ICO guidelines. In addition, where consent is relied upon for the processing of children's data, explicit consent will be required for this purposes.			
10	Data Breach	A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal details. This means that a breach is more than just losing personal data. Discussions with the Chief Digital Information Officer noted that information security breaches including data breaches are reported as detailed in the Security Incident Reporting Procedure. This information was then passed to the Police Lawyer (CDU) who will assess the breach and the necessity to inform the ICO. Review of the Security Incident Reporting Procedure confirmed that it set out the steps needed to detect; respond and recover from an incident, including a personal data breach. Following a recent breach at the Force, which was reported to the ICO, it was noted that the organisations have in place processes for investigating breaches, reporting to the ICO and notifying the data	The organisations will document plans to undertake the following: • Review all data breach procedures; • Include in the procedures the data protection officer to whom data breach will be reported; • Include in the procedures the types of data breaches as defined by the ICO; • Include procedures for reporting data breaches by third parties;	Police Lawyer (CDU) Head of Information Management	25th May 2018

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		subjects affected. There were also processes in place to ensure that there was audit trail showing inappropriate access to the organisations' systems. However, there was no documented plan in place to review the current processes and procedures to be in line with the GDPR. In particular the following steps should be undertaken: • Include in the procedures the data protection officer to whom data breach will be reported; • Include in the procedures the types of data breaches as defined by the ICO; • Include procedures for reporting data breaches by third parties; • Have mechanisms in place to ensure the organisations will report data breaches to the ICO within 72 hours where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach; and • Inclusion of the rule that failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.	• Have mechanisms in place to ensure the organisations can report data breaches to the ICO within 72 hours where the individual is likely to suffer some form of damage, such as through identity theft or a confidentiality breach; • Inclusion of the rule that failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself; and • Recruit an IT Security Officer (ITSO) to improve data breach processes, as a part of the planned ISMS development.		
11	Law Enforcement Directive (LED) / Data Protection Bill	The LED / Bill applies to 'competent authorities' who process personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. The Force had identified as part of its gap analysis the requirements of LED, however an action plan to address the following areas had not been formalised:	The Force will put in place comprehensive action plans to address the following activities: • Classification / identification of different categories of data subjects (such as victims, witnesses, offenders);	Police Lawyer (CDU) Head of Information Management	25th May 2018

Ref	ICO Area	Findings summary	Actions for management	Responsible owner	Implementation date
		• Classification / identification of different categories of data subjects (such as victims, witnesses, offenders); • Classification of whether the data is fact or personal opinion/assessment; e.g. witness statements vs. factual evidence; • Functionality of automated systems to ensure the Force is able to keep logs of processing operations in automated processing systems. This will include a log of any alterations to records, access to records, erasure and disclosures of records unless an exemption applies; • Review of procedures for transferring or sharing personal data across borders (either with relevant authorities or others) to ensure that they are compliant; and • Ensuring there is an appropriate policy in place for the sensitive processing of data. The extra categories of sensitive processing of data including genetic or biometric data would need to be included also.	• Classification of whether the data is fact or personal opinion /assessment; e.g. witness statements vs. factual evidence; • Functionality of automated systems to ensure the Force is able to keep logs of processing operations in automated processing systems. This will include a log of any alterations to records, access to records, erasure and disclosures of records unless an exemption applies; • Review of procedures for transferring or sharing personal data across borders (either with relevant authorities or others) to ensure that they are compliant; and • Ensuring there is an appropriate policy in place for the sensitive processing of data. The extra categories of sensitive processing of data including genetic or biometric data would need to be included also.		

APPENDIX A: SCOPE

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

Scope of the review

We will review the Force's and PCC's readiness for the implementation of the GDPR, in relation to the use of personal data, and the Police and Criminal Justice Data Protection Directive ('the Police Directive') in relation to the processing of personal data for preventing, investigating, detecting and prosecuting crimes.

1 Business processes and data discovery

Based on the documentation and information provided inspection of the management control processes designed to identify and document all in scope data across the organisations. Related data inflows and outflows focussing in particular on:

- the existence of process and data mapping.
- processes to classify data.
- identification of data flows to third parties.
- methods of data storage and transfer.

2 Third parties

Based on the assessment set out at (1), we will carry out the following:

- inspection of the methods used to identity third parties to whom the 'in scope' data is transferred.
- identification of methods used to assess contractual data confidentiality existence and coverage.

3 Data ownership

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

4 Data security system level controls

Tested data security controls agreed by you over data inflow, data repository and data outflow and report results by reference to recognised good practice.

5 Data storage and retention

Based on documentation and information at 1 above, commented on the existence of data retention and storage policies.

6 Awareness

Based on the documentation and information at 1 above, commented on the existence of GDPR awareness processes.

7 Data policy, roles and responsibilities

Based on the documentation and information at 1 above, commented on the existence and scope of current data policies.

Based on the documentation and information at 1 above, commented on the existence and designation of data protection roles and responsibilities.

Comment on current roles by reference to recognised good practice.

8 Individuals' rights

Based on the documentation and information at 1 above, commented on the existence of procedures for updating, deleting, and reporting personal data at department and organisation level.

9 Consent

Based on the documentation and information at 1 above, commented on the existence of processes in place to capture data consent.

10 Data breaches

Based on the documentation and information at 1 above, commented on processes in place for the detection, reporting and investigation of personal data breaches.

11 Police Directive

Review of how the organisation is proposing to take into account the changes to Police Directive as a result of GDPR.

Limitations to the scope of the audit assignment:

- The assignment has been delivered as 'agreed upon procedures' and therefore has not resulted in a formal assurance level or opinion.
- The scope of our work was limited only to those areas that have been examined and reported, and is not to be considered as a comprehensive review of all aspects of data protection.
- Any testing undertaken as part of this audit was on a sample basis.
- The information provided in the final report should not be considered to detail all errors or risks that may currently or in the future exist in data protection, and it will be necessary for management to consider the results and make their own judgement on the risks affecting the organisation.
- This report does not constitute legal advice; it is intended to provide advice on the suitability of internal controls in preparation for the GDPR requirements to be implemented mid-2018.

APPENDIX B: FURTHER INFORMATION

Persons interviewed during the audit:

- Force Solicitor and Head of Legal Services
- Interim Chief Executive Officer
- Police Lawyer (Civil Disclosure Unit)
- Head of Information Management
- Records Manager
- Chief Digital Information Officer
- Information Security Officer

Documentation reviewed during the audit:

- GDPR gap analysis
- Law Enforcement Directive Bill, September 2017
- Guidelines on Data Protection Impact Assessment (DPIA)
- Asset Register
- GDPR Working Group Terms of Reference
- Data Protection Officer job specification
- Information sharing agreement register
- Information Security Policy
- Records Management Policy
- Data Protection Policy

FOR FURTHER INFORMATION CONTACT

Dan Harris, Head of Internal Audit

Tel: 07792 948767

Daniel.Harris@rsmuk.com

Angela Ward, Senior Manager

Tel: 07966 091471

Angela.Ward@rsmuk.com

Philip Church, Client Manager

Tel: 07528 970082

Philip.Church@rsmuk.com