Final report v1.0

Findings from ICO consensual data protection audits and follow-up audits of police forces

Date issued: July 2021

ico.
Information Commissioner's Office

Contents

Introduction

The Information Commissioner's Office (ICO) is responsible for enforcing and promoting compliance with data protection legislation.

Audit has a key role to play in educating and assisting organisations to meet their obligations. Therefore, the ICO has undertaken a programme of consensual audits with police forces to:

- assess their processing of personal information; and
- provide practical advice and recommendations to improve the way they deal with information rights issues.

Following each police force audit, the ICO produced a bespoke audit report. Where we identified non-conformities with the data protection legislation, we made recommendations on how to improve compliance.

This report highlights the key findings and commonalities from 14 individual audit reports and 11 subsequent follow-up audits of police forces in England and Wales. It covers audits conducted between May 2018 to October 2020. It is intended to help police forces, and the wider criminal justice sector to see where they can make improvements in how they handle personal data. No individual organisation is named in the report.

Audit approach

The primary purposes of an audit are to:

- provide the ICO and police force with an independent opinion of the extent to which the police force is complying with data protection legislation;
- highlight any areas of risk to their compliance; and
- review the extent to which the police force demonstrates best practice in its data protection governance and management of personal data.

The audit scope is selected through a risk-based analysis of the organisation's processing of personal data, considering:

- cases referred to the ICO;
- internal intelligence; and
- issues with the sector and risks generally.

The final choice of scopes is mutually agreed with the organisation, prior to the audit.

Further information on the possible scope areas is explained in Appendix 1.

Each of the audits featured in this report covered a maximum of three scope areas. The governance and accountability scope was covered for most police force audits with additional scope areas selected as outlined above.

The table below summarises the scopes covered and the frequency.

Scope area	Frequency of scopes audited
Governance and accountability	13
Records management	4
Requests for personal data	5
Data sharing	4
Training and awareness	6
Information risk management	5
Personal data breach management and reporting	1
Information security	4

In advance of the site visit, the ICO reviewed the organisation's policies and procedures about the agreed scope areas. The methodology used by the audit team during the site visit was primarily desk-side interviews with key staff. The aim was to see how processes and policies work in practice to assess their operational effectiveness.

Since March 2020 on-site visits have not been possible due to the COVID 19 pandemic. Therefore, the ICO have carried out audits remotely using video technology to conduct interviews.

On completion of the audit, the ICO finalised the findings and recommendations in a formal report. The audit reports provided each police force with:

- an assurance opinion per scope area based on the work undertaken, using a framework of four categories of assurance, from high level of assurance to very limited assurance. More details of the assurance ratings are shown in Appendix 2;
- details of non-conformities and associated risk; and
- prioritised recommendations that may mitigate risks.

The police force was required to accept, partially accept, or reject the recommendations and complete an action plan indicating how, when and by whom they would implement the recommendations. The audit reports were

designed to be bespoke to the individual force and were not intended to be directly comparable.

Headline areas of risk

Common areas for improvement in the processing of personal data are outlined below, based on audit reports from the stated period. We have included some actual examples of practices we experienced during audits to highlight why we made our recommendations.

Governance and accountability - Record of processing activity

What is required

Police forces should keep an internal record of all processing activities (ROPA) they undertake, as well as any processors. This is in line with the requirements set out in Article 30 of the UK GDPR and DPA18 Part 3 (Law Enforcement Processing) section 61. This states that a ROPA must include:

- the name and contact details of the organisation (or other controllers, representatives and the DPO where applicable);
- the purpose of the processing;
- a description of the categories of individuals and of the personal data;
- the categories of recipients of the personal data;
- where applicable, details of the use of profiling;
- details of transfers to third countries including documenting the transfer mechanism safeguards in place;
- an indication of the legal basis for the processing;
- retention schedules; and
- a description of the technical and organizational security measures.

For more information, see Documentation | ICO; Article 30 (1) GDPR; Data Protection Act 2018 (legislation.gov.uk) Schedule 1

What we found

More than 75% of police forces audited either did not have a documented ROPA, or it was incomplete. In addition, the lawful bases for processing had not been determined in all cases. Some police forces were using the information asset register as a form of ROPA, but we did not consider that these provided the necessary level of detail as required by the data protection legislation.

Example

One police force had started, but not completed, an information audit which

required each department to identify how they collected information and whether they shared it. Therefore, the force did not have a full accurate register of the information they held or the lawful basis for processing personal data.

What we recommend
All police forces should ensure that they complete a ROPA that covers all processing activities. This is a requirement of the legislation (Article 30(1)) and it will also help to demonstrate compliance with other aspects of the data protection legislation.

For more information, see Documentation | ICO

When preparing to document processing activities in a ROPA, police forces should carry out a data flow mapping exercise (information audit). This will help to identify all current data processing activities. The data mapping should show what information is processed and document all the data that flows into, around and outside the organisation.

Governance and accountability – Data protection compliance and assurance

What is required
All organisations should document how they will:

- monitor adherence to the requirements and rules set out in their own policies and procedures. They should then ensure compliance with these requirements through physical routine compliance monitoring and the use of key performance indicators (KPIs); and
- conduct regular compliance checks on data processors (that process personal data on behalf of the organisation). For example, a local authority providing IT services. This should include the level and content of the data protection training the processor provides to their staff; the technical and organisational security measures in place; and whether the processor is complying with its specific legal obligations under the data protection legislation.

What we found
There was a lack of evidence within some forces that staff had received, read, and understood changes to key data protection policies and procedures.

KPIs were not being used to monitor information governance or data protection training completion or for records management (RM), including:

- file retrieval statistics;
- adherence to disposal schedules; and
- performance of the systems in place to index and track paper files containing personal data (see also Training and awareness).

Some forces were not undertaking routine data processor compliance checks to ensure that their processors had procedures to comply with their specific legal obligations under the data protection legislation. Compliance checks to assess completion of processor staff data protection training were also not being carried out in some cases.

What we recommend

Police forces should conduct routine compliance checks, on a force-wide basis, to test individuals' awareness and understanding of data protection policies and procedures. This will help to reduce the risk of personal data breaches.

Gathering of performance and compliance management information in the form of key performance indicators (KPIs) is a valuable tool. This will give forces oversight to understand and manage the effectiveness of the control measures in place. KPIs should have set targets in all key areas of information governance, including subject access requests (SARs), training, incident management and RM. Once forces set targets, they should continue to monitor performance against those targets and discuss them at senior management level to drive through improvements.

Compliance checks of data processors should include:

- an assessment of their information security (IS) arrangements;
- data protection training; and
- their awareness and understanding of data protection policies and procedures.

Training and awareness

What is required

A comprehensive data protection training programme is very important to ensure that all staff understand their obligations under the data protection legislation. It is an effective organisational measure to safeguard personal data and will create a culture of privacy across an organisation.

Article 24 UK GDPR and section 56 of the DPA18 requires organisations to implement appropriate data protection policies to:

- provide guidance for staff in their data protection legislation responsibilities; and
- demonstrate that processing is performed in accordance with the legislation.

These policies and procedures should form the basis for any staff training.

For more information, see Governance and accountability | ICO

What we found

Police forces rely on the National Centre for Applied Learning Technologies (NCALT) to provide e-learning courses on information management. The e-learning, although mandatory for all staff, is not sufficiently detailed for staff who process personal data on a regular basis or have specific data handling and IS management responsibilities. In several forces the training completion rates were not monitored using agreed KPIs (see also Governance and accountability).

We also found that staff who were designated as Information asset owners had not always received specific data protection training. This would support them in their role and ensure that information assets are managed and handled appropriately.

Example

One force had not completed a full training needs analysis (TNA). Consequently, front-line staff had not received training on how to redact personal information and staff in the force control room were referring to outdated legislation for access to personal information.

What we recommend

A TNA of all staff will help to identify those roles that involve handling sensitive or special category personal data or regularly interact with individuals that may need specific training.

Police forces should assign specialist training to individuals who have specific responsibilities for information management. For example, staff involved in:

- RM;
- IS;
- data protection (DP);
- disclosures;
- data sharing;
- personal data breaches; and
- data protection impact assessments (DPIAs).

This training will equip key staff with the detailed knowledge they need to fulfil their data protection responsibilities.

A TNA will help the organisation to identify and fill gaps from the general NCALT information management e-learning modules. They should refresh the training

on a regular basis. The use of KPIs will help senior management monitor adherence to data protection training completion (see also Governance and accountability)

Records management

What is required

Appropriate records management processes are required for managing both electronic and manual records containing personal data. This includes controls in place to monitor the creation, maintenance, storage, movement and destruction of personal data.

Individuals have the right to be informed about the collection and use of their personal data under Articles 13 and 14 of the UK GDPR and section 44 (1) of the DPA18. This is a key transparency requirement under the GDPR.

What we found

There were no regular checks on both in-house storage of records and third party records disposal facilities to ensure agreed standards were being met. We also found the whereabouts of physical records were not being adequately tracked.

Privacy notices were not comprehensive and clear to make individuals aware of:

- why their personal data was being processed;
- under what lawful basis their data was being processed; and
- what rights they had in relation to that processing.

Example

One force had no reliable way to track records that had been withdrawn from records storage. A record was not identified as missing until a new request was made to retrieve the record and it was then discovered that it was not available. The last known recipient was then contacted.

What we recommend

Police forces should schedule audits of in-house storage and any third party records disposal facilities. This will provide assurance that the organisations' agreed standards are being met.

They should employ robust tracking methods for physical records. Without robust tracking procedures the risk that the documents could be unlawfully accessed, compromised, or lost is greatly increased. Also, if there was a breach of special category data, the harm to the data subjects is substantially higher.

Police forces should make fair processing information available at the time of collecting data in the form of clear and comprehensive privacy notices. They

must actively provide this information by allowing individuals an easy way to access it.

Requests for access to personal data

What is required

The right of access, commonly exercised through a SAR, gives individuals the right to obtain a copy of their personal data as well as other supplementary information. This is an important right as it helps individuals to understand how and why organisations are using their data, and to check that they are doing so lawfully. Organisations must respond without undue delay and within one month.

The data protection legislation does not specify how an individual can make a valid request. A SAR can be made verbally or in writing (including through social media). Individuals can also make a request to any part of an organisation and they do not have to direct it to a specific person or contact point.

What we found

Not all forces had detailed procedures describing how they should manage requests for access. There was a lack of guidance on recognising requests, including verbal requests or requests received through unusual channels.

There were also a lack of quality assurance reviews. These would ensure that processes are followed, and that proper consideration is given to the removal of personal and third-party data when applying exemptions.

Performance in meeting the timescales for responding to SARs varied widely amongst police forces, but we found some were not meeting the statutory timeline.

Example

In one force, due to an increase in volume of SARs and limited resources, there was a backlog of SARs. This resulted in quality reviews of responses to requests for personal data not taking place.

What we recommend

Forces should make sure that they have suitable processes in place to record and handle all requests, regardless of the format that they are received in. They should have the necessary resources to respond to requests within the legal time limits.

They should ensure that all staff are aware of their obligations to treat verbal and written requests for personal data in the same way.

They should make sure that responses to requests are quality assured or dip sampled. This will help to ensure that they are applying the correct exemptions and following procedures.

Forces should provide more in-depth data protection training to individuals who are responsible for processing these requests.

Data sharing

What is required

When personal data is routinely shared it is good practice to have an information sharing agreement (ISA) in place to help demonstrate your accountability obligations. These agreements should be sufficiently detailed, and provide direction to all parties, to ensure the requirements of the data protection legislation are met. This should include how long an organisation will retain data for and how they will dispose of it at the end of the retention period.

Organisations should review ISAs on a regular basis to ensure routine sharing is as strictly controlled as possible.

They should have standardised, documented procedures in place for responding to ad hoc third party requests for personal data. They should keep records of responses, approval and quality assurance.

What we found

Police forces were not regularly reviewing ISAs to ensure the sharing continued to be necessary and complied with the data protection legislation.

We also found that procedures were lacking when it came to ad hoc disclosures. This included:

- a lack of quality assurance checks;
- insufficient recording of decisions not to share information; and
- a lack of checks to ensure that they were only sharing data still within the retention period.

What we recommend

Information sharing agreements set out a common set of rules to be adopted by the various organisations involved in a data sharing operation. These could well form part of a contract between organisations. It is good practice to have a data sharing agreement in place, and to review it regularly, particularly where information is to be shared on a large scale, or on a regular basis.

For ad hoc sharing, it may not always be possible to document the sharing in an emergency or time-dependent situation. However, it is good practice to make a record as soon as possible, detailing the circumstances, what information was shared and explaining why.

For more information, see Data sharing: a code of practice | ICO

Please note we have recently updated the code to include sharing personal data under the law enforcement processing provisions of Part 3 of the DPA18 and sharing between the UK GDPR/Part 2 DPA18.

Information risk management

What is required

A DPIA must be completed before an organisation begins any type of processing involving personal data that is "likely to result in a high risk" (Article 35 UK GDPR and section 64 DPA18). This means that although they have not yet assessed the actual level of risk, they need to screen for factors that point to the potential for a widespread or serious impact on individuals.

A DPIA should begin early in the life of a project, data sharing arrangement or change in processing. This should happen before organisations start processing and run alongside the planning and development process.

What we found

In general, forces were conducting DPIAs for new projects and processes. However, we found some forces were not instigating DPIAs when changes to existing processes or replacements to systems processing personal data occurred. In other forces we found that the DPIA procedure was not fully embedded into either the procurement or information sharing policies and procedures.

What we recommend

Police forces should ensure that they incorporate the requirement to undertake DPIA screening and completion into their local project management and procurement procedures, where appropriate. This includes when considering entering new data sharing arrangements. They should also ensure that replacement or changes to systems used to process personal data undergo DPIA screening.

For more information, see Data protection impact assessments | ICO and Article 35 UK GDPR

Information security

What is required
Organisations should have an IS policy to describe their approach and organisational measures to comply with the data protection legislation security principle. The policy and supporting procedures should provide guidance on:

- access control to systems holding personal data;
- reporting of IS incidents;
- protection against misuse or corruption during transportation; and
- what steps they will take to make sure the policy is implemented.

For more information, see Security | ICO

What we found
Not all forces had documentation to:

- describe procedures and processes used to secure personal data;
- incident management procedures; or
- the use of unencrypted media to store or transport personal data.

Access controls were not restricting an individual's login to different desktop computers at the same time. Regular user access rights checks were lacking which would help to ensure that the access rights are appropriate for the role and up-to-date.

Systematic clear desk sweeps or security spot checks were not being conducted by line managers or IS staff.

Example
In one force, regular clear desk sweeps and security checks were not being carried out consistently. Confidential waste bags containing personal data were left unsealed in rooms where ICO auditors were interviewing staff.

What we recommend
An up-to-date IS policy and associated procedures will provide guidance to staff, ensure compliance and satisfy the accountability principle of the data protection legislation.

For more information, see Accountability and governance | ICO

Staff allowed to use unencrypted media to store or transport personal data should receive instructions on the security measures that should be in place to protect the data from unauthorised disclosure.

Police forces should restrict access controls so that users may only log onto one desktop at a time. This prevents sharing of accounts and ensures that staff log off completely at the end of the shift or business day.

Forces should schedule compliance reviews of IS processes. This will identify IS issues and help prevent personal data breaches. The reviews should include adherence to access rights removal and changes, clear desk policy and encryption of removable media. Forces should document responsibility for completing these spot checks in the appropriate policies, procedures, and job descriptions.

Best practice seen during our audits (source: Audit Reports)

As a result of our audit engagements with police forces, we noted areas of good practice that occurred in one force or was a trend across several forces. Please note that the areas of good practice highlighted below were not present in all the police forces audited.

Training and awareness

- IAO training was developed, after identifying IAO needs and concerns through a questionnaire, along with an IAO handbook. The handbook identified and highlighted issues across a wide range of directorates and departments.
- Data Protection was classified as a "golden thread" and Learning and Development had incorporated it as a design principle throughout all internally developed and delivered training courses.
- Short videos were produced covering DP or Information Governance (IG) matters including; what is personal data, special category data, SARs, and data management. The short subject-focussed videos allowed staff to see, in a digestible format, their basic responsibilities under data protection legislation.

Governance and accountability

- The intranet had a means to flag and enforce a policy or guidance document that had to be read. This was done by a mandatory read receipt. If the item remained unread it was sent to the users email inbox.

- The Routine Orders function on the intranet was used to increase engagement and awareness of data protection. It was mandatory for staff to read the Routine Orders and, therefore, all staff members should have been aware of any changes to policies and updates to guidance.
- The appointment of clear desk champions ensured that areas which were not regularly visited by information management staff continued to engage fully with the clear desk policy. This also helped to raise staff awareness of IS procedures.
- Led by the DPO, the police force intranet was used to circulate a mixture of learning bulletins, short videos, new messages, policies or procedures, and trends in data breaches. Information bulletins were targeted at those involved with non-compliance. Maintaining a high-profile information governance campaign further elevated the importance of data protection compliance across the organisation.

Data sharing

- A Data sharing agreement register was put in place which recorded key details about each agreement, including the organisations involved, the data that was shared, and the legal basis for sharing.

Information risk management

- Information risks were recorded on one database. This provided access to both the local risk register, owned by each IAO, and the over-arching Force risk register. Risks were assessed locally using a risk matrix and those risks scoring higher than the threshold score appear on the Force risk register. The risk register was monitored by a dedicated member of staff who sent monthly reminders to review the information asset risk.

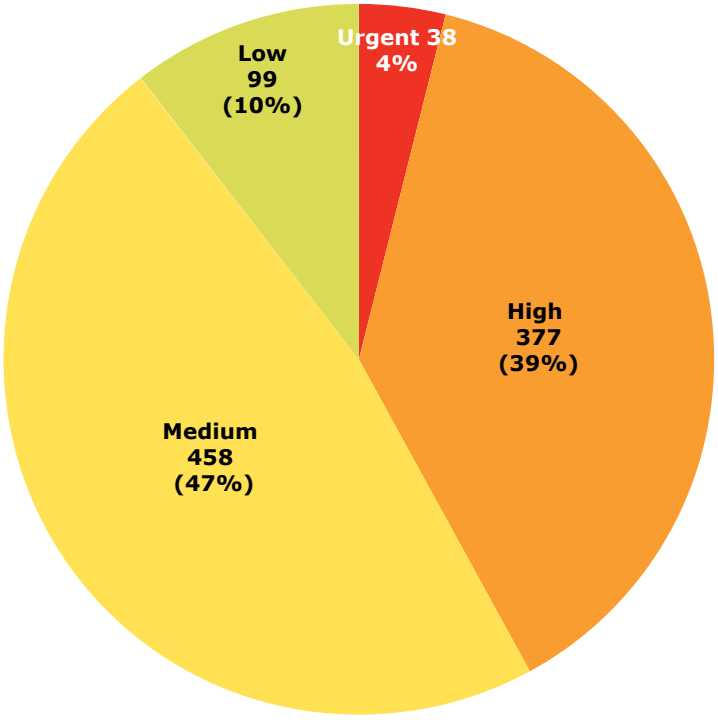
Recommendations made in our audits

Where we identified areas of weakness, including those outlined above, we made recommendations to assist the force to address them.

All recommendations were assigned a priority rating to indicate the risk to data protection compliance if they were not implemented: urgent; high; medium; and low. Appendix 3 shows the priority rating descriptions in detail.

We made 972 recommendations across the 14 police force audits. 4% (38) of these were assessed as urgent and 39% (377) were assessed as high priority.

Number of audit recommendations by priority rating (Source - audit reports)



85% (826) of the ICO audit recommendations were accepted by police forces, 11% (107) were partially accepted and actions to mitigate the risks were formally documented and agreed. 4% (39) of the recommendations were rejected. Police forces are at liberty to reject the ICO recommendations and accept the risk. However, should there be a subsequent data breach then this could impact any regulatory action taken by the ICO.

Follow-up audits (source: follow up audit reports)

When we issued the final report, we arranged a follow-up audit with each police force. This allowed the ICO to assess progress made against the agreed action plan. Follow-up audits took place between six to 12 months after the original audit report was issued.

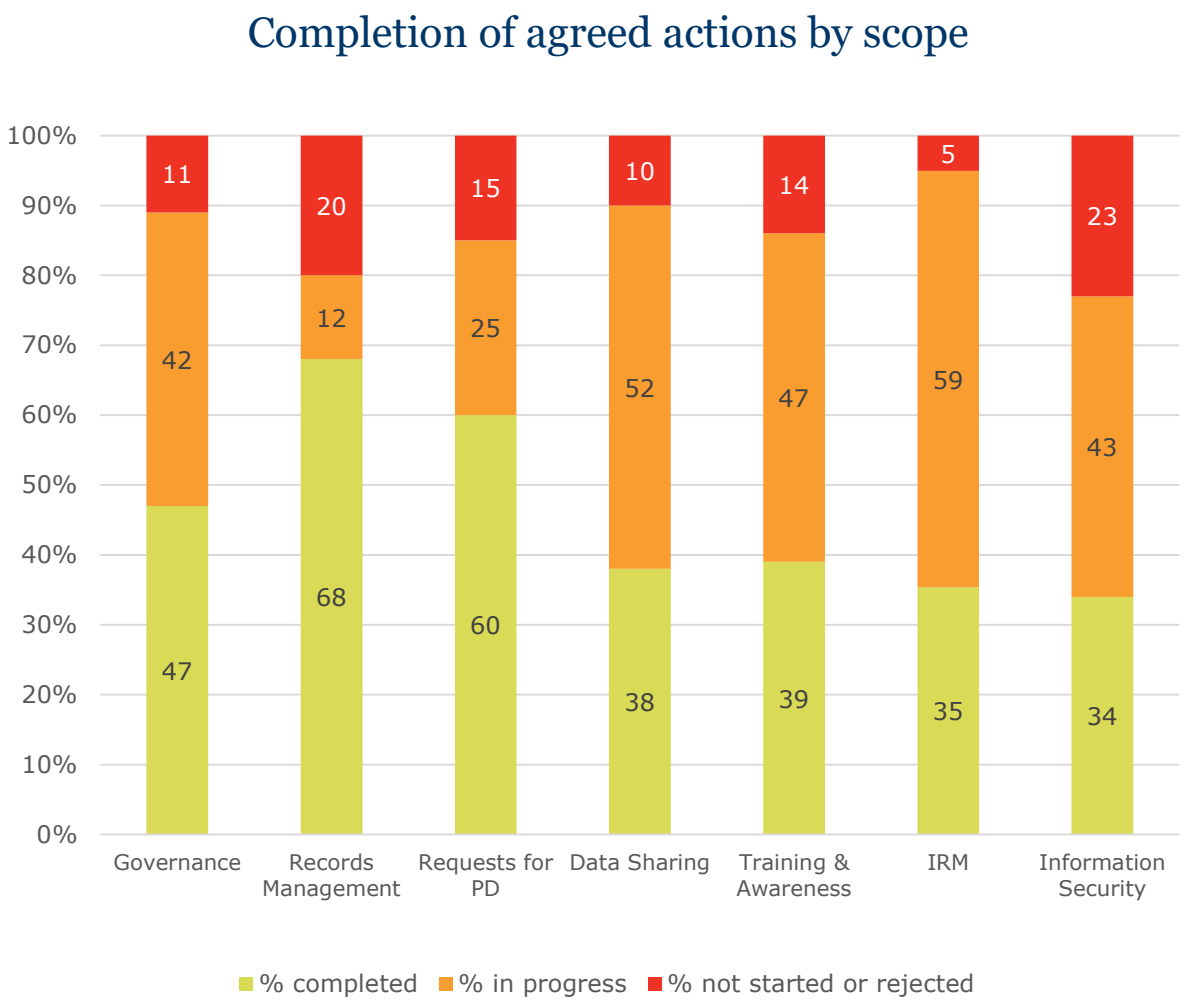
As part of the follow-up audit, each force was asked to assess their progress with the action plan by indicating whether they considered each action to be complete, in progress or not started. We requested that they provide supporting documentary evidence to demonstrate the actions they'd taken for the urgent and high priority recommendations from the original audit, as well as commentary on the action status of the medium and low priority recommendations.

The follow-up audit provided the ICO with a level of assurance that the agreed audit actions had been appropriately implemented. This mitigates the identified risks and thereby supports compliance with data protection legislation and implements good practice.

If there were any concerns with the lack of progress the Information Commissioner would consider whether it is appropriate to exercise her formal enforcement powers to ensure compliance with the data protection legislation.

Of the original 14 data protection audits, 11 follow up audits have been completed between June 2019 and October 2020.

Progress with agreed actions



Follow-up audit outstanding risks

The ICO assessed the completed action plan, evidence provided, and documented updates on the agreed actions. We found that on several occasions this differed considerably from the organisation's assessment. 77% of the urgent recommendations remained in progress and were not yet completed. It is the ICO's view that delaying completion of these urgent recommendations represents a significant risk to police forces and they should remain under review and should be managed appropriately. We would take the lack of progress into account if there was a personal data breach. It could potentially influence any of the ICO enforcement powers to ensure compliance with the data protection legislation.

The analysis of follow-up activity conducted to date highlights some key compliance areas where forces have struggled to mitigate the risks identified during our original audit activity. The following list includes the common areas of risk that are still outstanding:

Training and awareness

- The development of a TNA for all staff was still to be completed in some forces.
- There remained a lack of monitoring of completion rates for mandatory information management training and compliance of volunteers or contractors with the online e-learning NCALT training.

Records management

- Completion of a ROPA remained a challenge for many forces. It involves a detailed information audit, mapping of data flows and identifying information assets across the whole organisation. This can be time consuming.
- There was lack of clarity on identifying the lawful bases being relied on for processing personal data.

Governance and accountability

- Progress was incomplete with instigating procedures to confirm staff have read and understood key data protection policies after they have completed induction training or when changes to policies are made.
- There was insufficient monitoring of staff awareness and understanding of the forces data protection and IS policies.
- There was a lack of routine compliance checks of data processors against the terms of their contract and ensuring contracts are compliant with the provisions of the latest data protection legislation.
- Policies and procedures for access control, specialist training and DPIAs.
- Recommendations were rejected about internal audits of data protection practices. There was no formal internal audit plan covering information governance or data protection.

Data sharing

- Information sharing agreements were not routinely reviewed or had the necessary checks to ensure they were following the data protection legislation.

Information security

- There was a lack of policy for access controls.

- There remained an ability to login to more than one desk top computer.
- A physical register of IT equipment and removable media were not regularly checked.
- There was lack of controls on the return of IT hardware.

Request for personal data

- There was a lack of resourcing to handle and respond to SARs, both overdue and those that continue to be received. This could put pressure on meeting statutory timeframes.
- There was insufficient access to manual records to ensure requests for personal data could be responded to fully and within statutory timeframes.
- There was a lack of regular dip samples of cold cases relating to requests for personal data and conducting quality assurance checks before the response is sent to the requestor.
- There was a lack of documented procedures in place to monitor and analyse complaints made by data subjects on how their requests for personal data were handled.

Appendix 1 – Scope areas

Governance and accountability

The extent to which the following are in place and in operation throughout the organisation:

- information governance accountability;
- policies and procedures;
- performance measurement controls; and
- reporting mechanisms to monitor data protection compliance to both the UK GDPR and national data protection legislation.

Records management

The processes in place for managing both electronic and manual records containing personal data. This includes controls to monitor the creation, maintenance, storage, movement, retention and destruction of personal data records.

Requests for personal data

There are appropriate procedures in operation for recognising and responding to individuals' requests for access to their personal data.

Data sharing

The design and operation of controls to ensure the sharing of personal data complies with the principles of all data protection legislation.

Training and awareness

The provision and monitoring of:

- staff data protection;
- records management and IS training; and
- the awareness of data protection regulation requirements relating to their roles and responsibilities.

Information risk management

The organisation has applied a "privacy by design" approach. Information risks are managed throughout the organisation in a structured way so that management understands the business impact of personal data related risks and manages them effectively..

Personal data breach management and reporting

The extent to which the organisation has measures in place to:

- detect, assess and respond to security breaches involving personal data;
- record them appropriately; and
- notify the supervisory authority and individuals, where appropriate.

Information security

There are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.

Appendix 2 – Assurance ratings in individual scope areas (source audit report executive summary)

Number = numbers of police forces

Scope Area	High	Reasonable	Limited	Very limited
Governance and accountability	0	8	5	0
Records management	0	2	2	0
Requests for personal data	0	2	3	0
Data sharing	0	5	0	0
Training and awareness	1	4	2	0
Information risk management	3	2	0	0
Personal data breach management and reporting	0	1	0	0
Information security	1	4	0	0

Key:

High: There is a high level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified only limited scope for improvement in existing arrangements and as such it is not anticipated that significant further action is required to reduce the risk of non-compliance with data protection legislation.

Reasonable: There is a reasonable level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified some scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

Limited: There is a limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified considerable scope for improvement in existing arrangements to reduce the risk of non-compliance with data protection legislation.

Very limited: There is a very limited level of assurance that processes and procedures are in place and are delivering data protection compliance. The audit has identified a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

Appendix 3 - Recommendation priority ratings descriptions

Urgent Priority Recommendations
These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.

High Priority Recommendations
These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.

Medium Priority Recommendations
These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.

Low Priority Recommendations
These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.

Further reading

1. Guide-to-data-protection-audits.pdf (ico.org.uk)
2. Data sharing: a code of practice | ICO
3. Individual rights | ICO
4. Accountability and governance | ICO
5. Audits and overview reports | ICO