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

Date issued: September 2023

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 organisations in the criminal justice sector 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 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 16 individual audit reports and 9 subsequent follow-up audits of organisations in England and Wales. It covers audits conducted between October 2020 to March 2023. It is intended to help organisations, 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 organisations with an independent opinion of the extent to which the organisation is complying with data protection legislation;
- highlight any areas of risk to their compliance; and
- review the extent to which the organisation 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 table below summarises the scopes covered and the frequency.

Scope area	Frequency of scopes audited
Governance and accountability	13
Records management	6
Requests for personal data	2
Data sharing	3
Training and awareness	5
Information risk management	4
Personal data breach management and reporting	3
Information security	3
Role of the DPO	2
Remote Working & BYOD	2
Processor, Third Party Supplier and Controller Relationship Management	1

In advance of interviews with key staff, which took place either remotely or as part of a site visit, the ICO reviewed the organisation's policies and procedures about the agreed scope areas. The aim of interviews was to see how processes and policies work in practice to assess their operational effectiveness.

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

Each organisation was required to accept, partially accept, or reject the recommendations and complete an action plan indicating how, when and by

whom the recommendations would be implemented. The audit reports were designed to be bespoke to the individual organisation 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 encountered during audits to highlight why we made our recommendations.

Governance and accountability - Record of processing activity

What is required
Police forces and criminal justice agencies must keep an internal record of all processing activities (ROPA) they undertake, as well as any activities undertaken by 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 90% of organisations audited either did not have a completed documented ROPA, or it was insufficient. In addition, some of the required details such as the lawful bases for processing had not been determined in all cases. Some organisations 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
Several organisations 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 organisation did not have a full accurate register of the information they held or record of the lawful basis for processing personal data.

What we recommend
All police forces and criminal justice agencies 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, organisations 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 organisations that key data protection policies and procedures were in place, kept up to date, and communicated to staff.

Most organisations were not regularly using KPIs 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).

Where organisations did have KPIs in place, these were not always reported at Board level, resulting in a lack of oversight, with particular regards to Records Management. Some organisations had a focus on reporting KPIs for Subject Access Requests (SARs) and Freedom of Information (FOI), but this same level of reporting was not always in place for training figures or Records Management.

Many organisations 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.

For these compliance checks to be effective, some organisations also needed to ensure that they had sufficient written contracts in place with all data processors, and that these were being regularly reviewed to confirm they met all data protection legislative requirements.

What we recommend
Organisations should make sure they have appropriate policies and procedures in place that cover all key data protection areas. They should conduct regular compliance checks across their organisation, to test individuals' awareness and understanding of these. 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 organisations 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 organisations 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.

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 often 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 and retrieval of physical records were not always being adequately tracked through the use of KPIs and compliance checks (see Governance and Accountability).

Privacy notices were often 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.

Many organisations also did not have a sufficient Appropriate Policy Document (APD), which clearly outlined compliance measures and retention policies for special category and criminal offence data.

What we recommend
Organisations 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.

Organisations 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 Subject Access Request (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 organisations had detailed procedures describing how they should manage requests for access with regards to Data Protection legislation. There was a lack of guidance on recognising requests, including verbal requests or requests received through unusual channels.

There was also a lack of guidance and clarity around the required supplementary information that must be provided alongside any copies of personal data requested. This must be sufficiently granular and specific to the data subject that made the request to ensure compliance with Article 15 of the UKGDPR and Section 45 of the DPA18.

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

What we recommend
Organisations 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.

Organisations should provide more in-depth data protection training to individuals who are responsible for processing these requests. This should include their responsibility to provide privacy information when responding to data 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 appropriate direction to all parties, to ensure data protection requirements are met. This should include the security measures in place, as well as how long an organisation will retain data for and how they will dispose of it at the end of the retention period.

Organisations should regularly review ISAs to ensure they continue to have the necessary controls in place for routine sharing.

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
Organisations did not review the sharing of personal data to ensure the appropriate agreements were in place. Where ISAs were held, they were not regularly reviewed to ensure the sharing continued to be necessary and complied with the data protection legislation.

We also found that some organisations did not have procedures on how to deal with ad hoc disclosures.

What we recommend
Information sharing agreements set out standardised rules to be adopted by the various organisations involved in a data sharing operation. These could potentially 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.

Organisations should have processes in place for the handling of ad hoc data sharing. This should include the verification of identity and lawful basis, ensuring the data is within the retention period, and the logging of decisions not to share. It may not always be possible to document ad hoc 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, or any exemptions applied.

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

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 several organisations had not completed a Training Needs Analysis (TNA) to determine what learning is required for specific roles involved in the collection of processing of personal data. For example, staff who were designated as Information Asset Owners (IAOs) 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.

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. This would then help to determine the specific training that may be beneficial.

Organisations 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 properly perform their data protection responsibilities.

A TNA would help the organisation to identify and fill gaps from the general NCALT information management e-learning modules. Training should be refreshed on a regular basis. The use of KPIs will help senior management monitor adherence to data protection training completion (see also Governance and accountability).

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 before assessing the actual level of risk, the organisation must screen for factors that point to the potential for significant or extensive 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, feeding into the decisions made along the way.

What we found
In general, organisations were conducting DPIAs for new projects and processes. However, we found that many organisations did not have the requirements for DPIA completion integrated into their relevant policies and procedures, such as Change Management Processes. In other organisations, we found that DPIAs were lacking in necessary detail, particularly around defining the controller/processor relationship with third parties. Organisations also did not have processes in place for regularly scheduled reviews of DPIAs, which chances new potential risk areas not being recognised and mitigated accordingly.

What we recommend
Organisations should ensure that the requirement to undertake DPIA screening and completion is integrated into their project management and procurement

procedures, as well as relevant data protection-related policies. This includes when considering entering new data sharing arrangements. Decisions not to undertake a DPIA should also be recorded. Organisations should also ensure that DPIAs are of sufficient detail to meet legislative requirements and are subject to a regular formal review process.

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

Personal data breach management and reporting

What is required
Organisations should have a data breach management policy and procedure to outline how staff handle any breaches or near-miss incidents. The policy and supporting procedures should provide guidance on:

- duty to report certain types of personal data breach to the ICO within 72 hours;
- informing the individual affected;
- detection, investigation and internal reporting procedures; and
- keeping a record of any personal data breaches.

What we found
Not all organisations had documented procedures to guide staff on formal reporting mechanisms required for personal data breaches. There was also a lack of adequate guidance staff with responsibility for personal data breach management, including near miss incidents. This included a lack of clarity around out of hours reporting processes.

What we recommend
Organisations should have allocated responsibility for managing breaches to a suitably trained dedicated person or team. They should also have an up-to-date personal data breach policy and associated procedures which provide guidance to staff, and ensure compliance with reporting requirements. These should include:

- recognising a personal data breach;
- internal process for recording all breaches, including those that don’t need to be reported;
- how to escalate a security incident to the appropriate person or team to determine whether a breach has occurred;
- formal mechanisms for reporting relevant data breaches to the Information Commissioner; and

- process to assess likely risk to individuals as a result, and notifying affected individual without undue delay.

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

Organisations are also required to ensure that they keep logs of actions on any automated processing systems they operate. These should include at least the following:

- collection;
- alteration;
- consultation;
- disclosure (including transfers);
- combination; and
- erasure.

For more information, see Logging | ICO

What we found
Not all organisations 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 or used for remote working.

Guidance did not adequately cover processes for reporting data breaches internally, to the ICO, or to data subjects. Organisations needed to implement or review controls around the use of mobile devices, including laptops and mobile phones, for remote staff. Access controls did not always include physical access

to secure areas, and Joiners, Movers, Leavers policies. 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 regularly being conducted by line managers or IS 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, including when working remotely, should receive instructions on the security measures that should be in place to protect the data from unauthorised disclosure. Compliance checks should be done to provide assurance that this guidance is being followed.

Organisations should restrict access controls so that users may only access both physical and digital areas that are suitable for their roles and responsibilities.

Organisations 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.

Systems must be put in place to ensure that automated processing systems have logging capabilities. This will ensure that organisations are able to monitor and audit internal processing within these systems. It will also enable monitoring of inappropriate access or disclosure of data.

Role of the DPO

What is required
Organisations should have a dedicated Data Protection Officer (DPO) in compliance with Article 37 of the UK GDPR. The DPO should:

- assist the organisation in monitoring internal compliance;
- inform and advise on data protection obligations;
- provide advice regarding Data Protection Impact Assessments (DPIAs); and
- act as a contact point for data subjects and the ICO.

The DPO must be independent, an expert in data protection, adequately resourced, and report to the highest management level.

For more information, see Data Protection Officers | ICO

What we found
Not all organisations had appropriately assigned tasks to the DPO, as stipulated in section 71 of the DPA18, such as data protection training and conducting audits. Organisations did not have sufficient dedicated resource from the DPO, or appropriately resourced operational roles in place to support the management of IG and DP. Where the DPO advised on DPIAs, their input was not always formally recorded to assist project managers in implementing any recommendations.

What we recommend
Organisations should ensure they have adequate resource from their DPO, with sufficient support in place to assist in the daily management of IG and DP throughout the organisation. The DPO should be involved in all issues relating to the protection of personal data, in a timely manner. The tasks assigned to DPOs should include:

- monitoring compliance with the UK GDPR and other data protection laws, internal data protection policies, awareness-raising, training and audits;
- acting as point of contact for the ICO as well as data subjects and employees;
- advising on DPIAs, and monitoring their progress; and
- having due regard to the risk associated with processing operations.

Organisations should also ensure that the contact details of the DPO are published in order to make them easily accessible to data subjects.

Remote working and Bring Your Own Device (BYOD)

What is required
Organisations should have governance and processes in place for managing personal data which is accessed remotely or through staff members' own devices. This should include controls to monitor hardware issued for remote working, staff owned hardware where company personal data is accessed, access and system controls, risk management and staff training.

What we found
Not all organisations had sufficient controls in place around the use of mobile devices or the use of social media for work related tasks. There was a lack of clear processes to regularly review access controls, including privileged access rights, across the systems in use. There were also not satisfactory controls

documented around the use of social media, such as WhatsApp, for work related tasks including the sharing of personal data.

What we recommend
Organisations should put in place appropriate security controls for home or remote working, together with guidance for staff on their responsibility to keep personal information secure. They should also implement controls around the use of mobile devices, including both laptops and mobile phones, for staff who work remotely.

Organisations should ensure they establish and monitor compliance with policy around the use of social media for work related tasks. The policy should be communicated to staff with checks on compliance proportionate to the risk. They should implement a regular review of access controls, including a Joiners, Movers, Leaver's policy.

This will help organisations gain assurance that staff who work remotely are not putting personal information at increased risk by their use of mobile devices and social media.

Processor, third party supplier and controller relationship management

What is required
Organisations should ensure there are effective relationship management controls in place with all processors and third party suppliers. Whenever a controller uses a processor, there must be a written contract (or other legal agreement) in place. The contract must outline the responsibilities and liabilities of both parties. If a processor uses another organisation to assist in its processing of personal data for a controller, it needs to have a written contract with that sub-processor.

The contract must set out details of the processing including:

- the subject matter of the processing;
- the duration of the processing;
- the nature and purpose of the processing;
- the type of personal data involved;
- the categories of data subject; and
- the controller's obligations and rights.

- For more information, see Contracts | ICO

What we found
As referenced in Governance and Accountability above, many organisations did not have a RoPA in place, informed by data mapping activities. Without this, organisations can not have assurance that all processors had been identified and had a contract in place.

What we recommend
Organisations should ensure that they complete data mapping across the organisation, and as part of this they should identify all processors in place. Once processors have been identified and documented, organisations should ensure that they have suitable contracts or agreements in place, which outline the relationship and responsibilities of each party. These contracts and agreements should be regularly reviewed, alongside the RoPA, in order to ensure that the correct controls remain in place for the processing taking place.

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

As a result of our audit engagements with organisations, we noted areas of good practice that either occurred in one organisation or were seen across several organisations. Please note that the areas of good practice highlighted below were not present in all of the organisations audited.

Governance and accountability

- Several organisations had established robust processes for ensuring that policies and procedures were reviewed in accordance with scheduled review dates. Adherence to the review date was overseen and monitored quarterly via a KPI. A process was also in place for escalation where non-compliance occurred, and the ICO noted a marked improvement in compliance.

Data sharing

- DPIA templates had been included as an appendix to an information sharing agreement (ISA) template. This helped to ensure that DPIA screening, or completion, was undertaken for all proposed new data sharing arrangements to identify risks, benefits and appropriate controls.
- The use of a comprehensive contract performance tracker to manage, and risk assess all contracts enabled organisations to gain assurance that data processors and third-party suppliers continue to perform at the correct level and identify new risks. The tracker included: a risk assessment which drives the frequency of 'supplier' checks; high risk contracts for critical suppliers and/or data processors checked monthly; inclusion of ISO27001 requirements in the assurance framework for high-risk contracts; results of annual checks recorded; a dashboard function to show the performance

of 'suppliers' based on the assessed scores; dates for contracts due to expire and those expired; the dashboard used as a reporting tool.

Information risk management

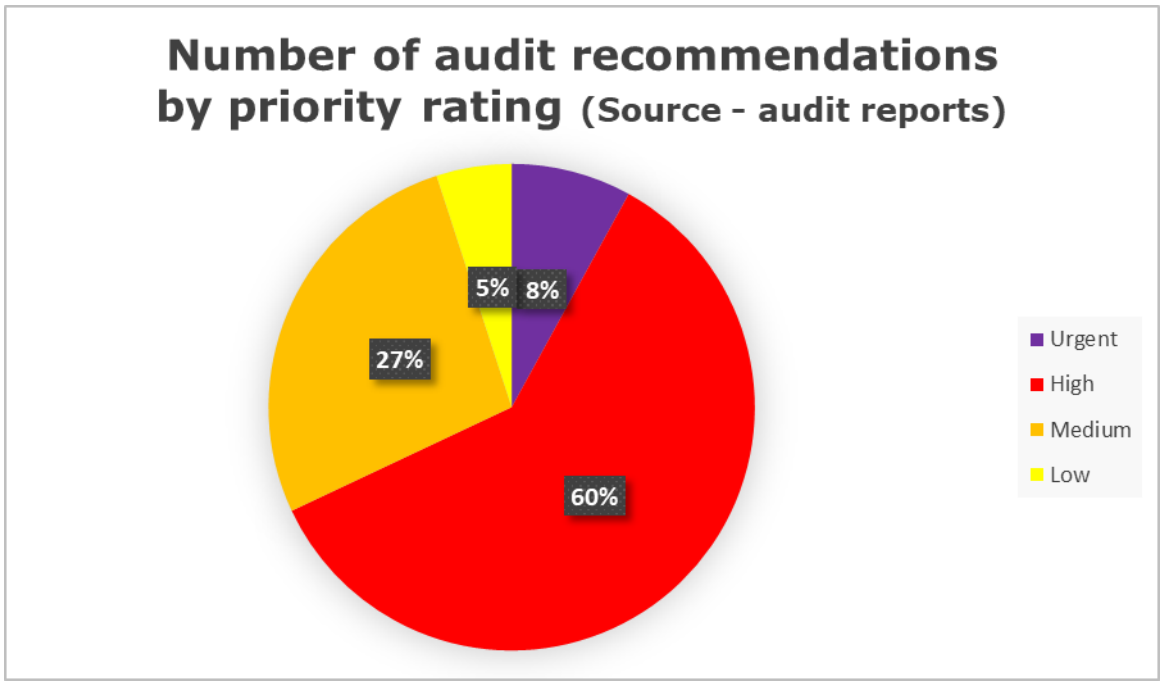
- Some organisations had conducted quarterly reviews of information assets with their data guardians. As well as identifying and mitigating information risks, the reviews were used to highlight any up and coming new initiatives or projects that may require a DPIA.

Recommendations made in our audits

Where we identified areas of weakness, including those outlined above, we made recommendations to assist the police force or criminal justice agency 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 1075 recommendations across the 16 audits. 8% (89) of these were assessed as urgent and 60% (654) were assessed as high priority.



83% (885) of the ICO audit recommendations were accepted by organisations, 14% (156) were partially accepted and actions to mitigate the risks were formally documented and agreed. 3% (35) of the recommendations were rejected. Organisations are at liberty to reject the ICO's lower priority 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 and agreed action plan, we arranged a follow-up audit with each organisation. This allowed the ICO to assess progress made against the agreed action plan. Follow-up audits typically took place between six to 12 months after the original audit report was issued.

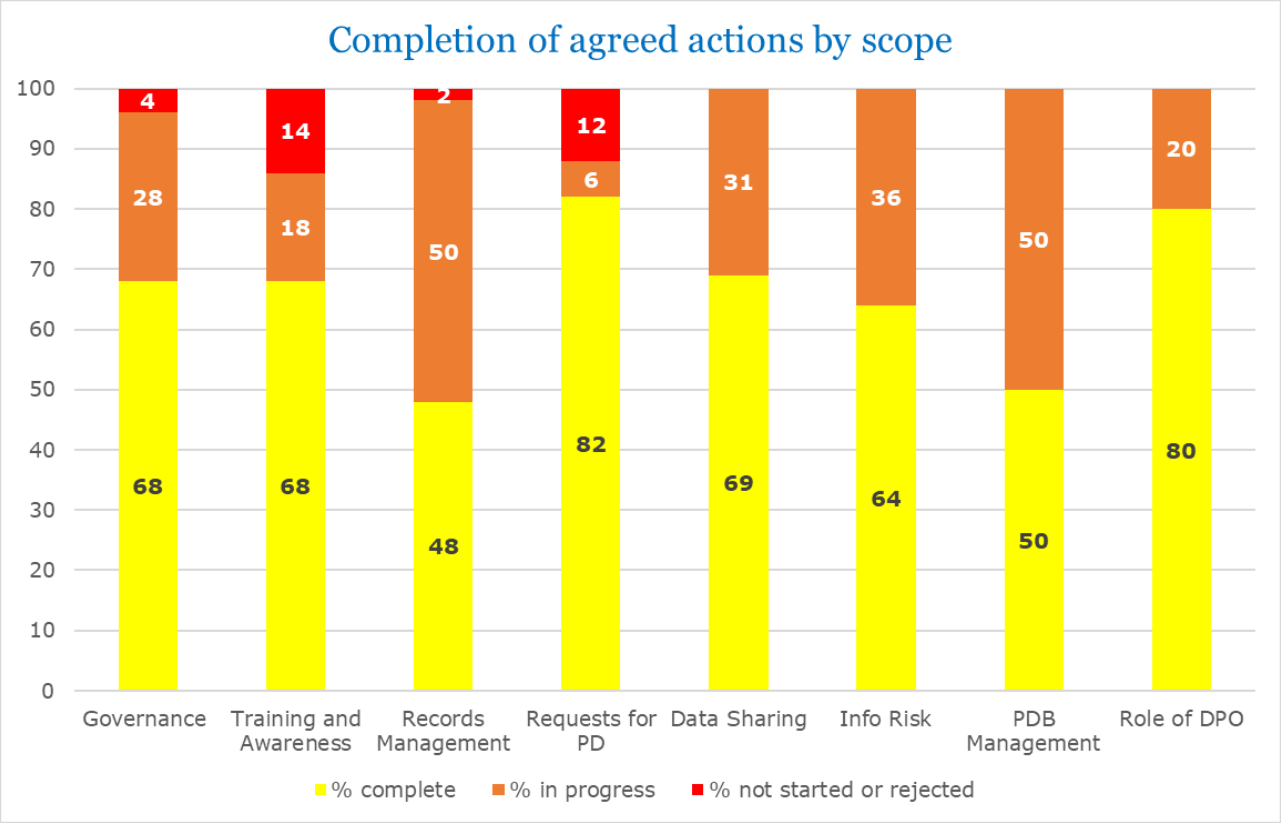
As part of the follow-up audit, each organisation was asked to assess their progress with the action plan by indicating whether they considered each action to be complete, in progress or not started. We requested that they provide supporting documentary evidence to demonstrate the actions they had taken 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 his formal enforcement powers to ensure compliance with the data protection legislation.

Of the original 16 data protection audits, 7 follow up audits were completed between November 2021 and December 2022.

Progress with agreed actions



The Records Management scope had the lowest percentage of completed actions at 48%, while Requests for Personal Data and Role of the DPO both had a majority completed. There remained actions either yet to be started or rejected in four scopes: Governance and Accountability; Training and Awareness; Records Management, and Requests for Personal Data.

Follow-up audit outstanding risks

The ICO assessed the completed action plan, evidence provided, and documented updates on the agreed actions. 55% of the urgent recommendations accepted by organisations remained in progress and were not yet completed at the time of the follow up. It is the ICO's view that delaying completion of these urgent recommendations represents a significant risk to organisations and they should remain under review and should be managed appropriately. We would take the lack of progress into account if the organisation was to subsequently suffer a personal data breach and it could potentially influence any decision in relation to the application of the ICO's enforcement powers.

The analysis of follow-up activity conducted to date highlights some key compliance areas where organisations 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:

Governance and accountability

- Progress with data mapping and implementing an effective RoPA was incomplete.
- Organisations were still working to gain assurance that staff have read and understood key policies and procedures.
- Fully incorporating DPIA requirements into project and change management procedures remained in progress.
- Organisations were yet to implement a programme of internal and external audits of data protection practices.

Records management

- As above, completion of a RoPA remained a challenge for many organisations. 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.
- Conducting data quality reviews of records held both physically and electronically was still underway.

Request for personal data

- Due to incomplete data mapping and RoPAs, potential inaccuracies remained within Privacy Notices.

Data sharing

- The outstanding work on data flow mapping meant that there could not be assurance that all routine data sharing arrangements were supported by written agreements.

Training and awareness

- Development of KPIs for training completion monitoring was still in progress.

- Some organisations were yet to document a Training Needs Analysis to determine training requirements throughout the organisation.

Information Risk Management

- Policies and procedures did not all make reference to DPIA requirements.

Personal Data Breach Management and Reporting

- Policies and guidance around data breaches and incident reporting remained in progress for some organisations.

Role of the DPO

- Some organisations still faced problems in ensuring their DPO was sufficiently resourced to fulfil their role sufficiently and meet legislative requirements.

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.

Role of the DPO

The extent to which the organisation has complied with their obligations under UK GDPR to appoint an independent DPO who is properly trained and resourced.

Remote Working and Bring Your Own Device

The governance and processes in place for managing personal data which is accessed remotely or through staff members' own devices. This will include controls to monitor hardware issued for remote working, staff owned hardware where company personal data is accessed, access and system controls, risk management and staff training.

Processor, Third Party Supplier and Controller Relationship Management

Organisations should ensure there are effective relationship management controls in place with all processors and 3rd party suppliers. Written contracts between controllers and processors are a requirement under the UK GDPR. These contracts must now include specific minimum terms. These terms are designed to ensure that processing carried out by a processor meets all the UK GDPR requirements, not just those related to keeping personal data secure.

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

Number = numbers of organisations

Scope Area	High	Reasonable	Limited	Very limited
Governance and accountability	0	4	9	0
Records management	0	2	4	0
Requests for personal data	0	1	1	0
Data sharing	0	1	2	0
Training and awareness	0	2	3	0
Information risk management	0	4	0	0
Personal data breach management and reporting	0	2	1	0
Information security	0	1	2	0
Role of the DPO	1	1	0	0
Remote Working & BYOD	0	2	0	0
Processor, Third Party Supplier and Controller Relationship Management	1	0	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