Information Governance Compliance Review

Compliance Programme - Year Two Report

North Yorkshire Fire and Rescue Service

For: SIRO

Status: Final Report

Date Issued: 19th September 2021

Contents

1) Introduction and Scope

Background

In May 2018 the UK adopted the General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 18) as its primary data protection legislation replacing the Data Protection Act 1998. This new legislation:

- Promotes enforceable accountability
- Provides greater rights for individuals
- Recognises the advances of privacy intrusive technology

One of the biggest changes to the legislation was that for the first time certain organisations were required to appoint a statutory data protection officer (DPO). The DPO needs to have expert knowledge of information governance legislation and best practice but is also required to be independent from the decision-making process within the organisation.

From April 2018 Veritau officially launched its DPO service and provided organisations with a number of resources in order to assist in ensuring compliance with the new tougher Data Protection requirements. This included, amongst other things, a consultancy visit, provision of guidance, and the provision of template documents that could be adopted by organisations. As part of the service Veritau conducted an Information Governance Audit and submitted the findings of that audit in the format of a report.

Following the UK's exit from the European Union, the UK adopted the UK GDPR to serve the purpose previously adopted by the GDPR.

Veritau provides this DPO service to NYFRS and, as your appointed DPO, Veritau is responsible for supporting NYFRS in achieving compliance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 18). This compliance review is designed to determine the extent of current compliance with the data protection legislation and highlight any areas of good practice or risks of non-compliance. Areas of weakness are identified and Veritau will provide guidance to ensure that, going forward, NYFRS meets the requirements of the UK GDPR and the DPA 18.

The Compliance Review is also an opportunity to collate all the data protection information for the senior leadership of an organisation, and enhances business continuity. NYFRS has supported the development of this review by completing a desk-based questionnaire and providing requested documents.

The Compliance Review programme has multiple stages to cover various compliance objectives and ensure that compliance is continuing. Compliance with Data Protection legislation, other relevant legislation and practices is a continuing exercise and even after the programme is completed organisations must be careful to ensure that the legislation is still adhered to. The programme will evolve to suit the changing landscape of data protection legislation and to suit the needs of Veritau's clients. However, the planned contents of the review are included below:

First Year Compliance Review

The First Year Compliance Review will feature questions on:

- ICO Registration
- Governance and Accountability
- Information Governance Policies
- Privacy Notices
- Websites, Social Media and Cookies
- Information Asset Management
- Data Protection Impact Assessments
- Contracts
- Information Sharing
- Lawful Basis for Processing Personal Data
- Consent
- Children's Online Services
- Direct Marketing

- Data Subject Rights
- Records Management
- Training
- Security of Personal Data
- Information Security Incidents
- Surveillance

Second Year Compliance Review

The Second Year Compliance Review will feature the same questions as the previous year, but will also expand upon the sections on:

- Information Governance Policies
- Information Asset Management
- Data Protection Impact Assessments
- Contracts
- Lawful Basis for Processing Personal Data
- Security of Personal Data
- Information Security Incidents

Third Year Compliance Review

The Third Year Compliance Review will feature the same questions as the previous year, but will also expand upon the sections on:

- Information Asset Management
- Data Protection Impact Assessments

- Records Management
- Information Security Incidents

2) Review

2.1 ICO Registration

NYFRS has registered with the ICO as tier 3. The certificate is annotated with the statement of being subject to the Freedom of Information Act. A member of staff has been given specific responsibility for ensuring the registration has been renewed.

2.2 Governance and Accountability

NYFRS has selected the DCFO as Senior Information Risk Owner (SIRO). The Senior Information Risk Owner has responsibility for understanding how NYFRS's aims may be effected by information risk and make decisions based on business need and the data protection officer's advice. Information risks are included on NYFRS's risk register.

NYFRS has a corporate information governance group (CIGG) or equivalent. They meet monthly, appropriately senior staff do sit on the group (Including the DCFO, and heads of function). There is a Terms of Reference document, it is adequate. Performance statistics are reviewed by the CIGG equivalent. There is a system in place for operational staff to raise data protection issues and risks.

2.3 Information Governance Policies

NYFRS does not have an information governance framework or equivalent. NYFRS has not got an information governance strategy that which outlines responsibilities, strategic responsibilities and includes a policy overview.

NYFRS has the following information governance policies: CCTV Scheme, Data Protection Policy, Data Subject Rights Request Procedure, FOI and EIR Policy, Information Security and Handling Policy, Information Security Incident Management Policy, Records Management Policy.

However, the following policies require revisions (further advice surrounding these policies has been provided in the summary of recommendations section): CCTV Scheme, FOI and EIR Policy, Records Management Policy.

NYFRS does not have these recommended polices: Special Category Data Policy

Existing policies do have an agreed format and style, they do have version control. Policies have been signed off by appropriate senior officers. Policies have been added to the review cycle.

The following policies have been reviewed this year: Data Protection Policy

The following policies are scheduled to be reviewed this year: FOI and EIR Policy, Information Security and Handling Policy (The "next review" and "last review" section on the front page of this document have not been updated, however the Document Change history section records the last review as 15/01/2019).

Policies are stored on the NYFRS intranet which appears to be suitably accessible to employees. New policies and/or changes to policies have been suitably communicated to employees through staff bulletins.

2.4 Privacy Notices

NYFRS has the following privacy notices: CCTV, Creditors and Debtors, Emergency Incidents, Fire Investigations, Home Fire Safety / Safe and Well Visits, Photographs and Videos, Recruitment and Selection, Staff, Technical Fire Safety and Site Specific Risk Information, Website and Social Media.

However, the CCTV Privacy Notice will need the retention period section reviewing as detailed in the summary of recommendations section below. I would also advise that the privacy notices as a whole are reviewed to ensure matching format and to ensure the DPO contact details are included on every notice.

NYFRS requires the following privacy notices: Youth Engagement Privacy Notice.

NYFRS has adopted 'just in time' notices on data collection forms. The provided example notice does state the purpose and link to an appropriate privacy notice.

2.5 Websites, Social Media and Cookies

The NYFRS new website does have a cookie banner to allow users to select what cookies to allow. NYFRS has a Facebook page. I would recommend that a link to the Website and Social Media Privacy Notice is included in the 'about' section of the Facebook page.

2.6 Information Asset Management

NYFRS maintains an information asset register (IAR). Veritau has reviewed this document and has recommendations, which can be split into two types: recommendations to meet minimum ROPA requirements, and recommendations to meet best practice.

1) Recommendations to meet minimum ROPA requirements:

- The "purpose" of the asset, and the "description" are mandatory fields. The NYFRS asset register does have these fields, but they would benefit from some enhancement. The ROPA should function as a business continuity document, and also should be able to be provided to the ICO upon request, this means the document should be mostly standalone and the description or purposes shouldn't require further explanation e.g. Asset 44 – The "Vision System" - it isn't clear to me as an 'outsider' what this asset is.

  I recommend the next time this is reviewed it is done so with the thought of whether an ICO case officer or even a member of the public unconnected to how NYFRS works, would understand.

- The ICO specify that there should be a "details of transfers to third countries" section. If NYFRS doesn't transfer any personal data to third countries I would recommend that a column is still added to make this clear.
- The ICO specify that the ROPA includes a description of the technical and organisational security measures.

2) Recommendations to meet best practice:

- The ROPA should document the lawful basis (Article 6 and Article 9 Conditions of the UK GDPR).
- Where consent is used, the ROPA should document how consent is sought and where evidence of consent is kept.
- The ROPA should include a column to record any personal data breaches affecting an asset.
- The asset should include a retention period or indicate where the retention periods can be found.

The IAR has not been kept up to date, e.g. we have been informed that all data processor agreements have been checked, however the asset register has many of these listed as not yet checked.

Information Asset Owners are aware of their responsibilities. The IAR is reviewed annually (or when a significant change is to be made) and the CAO Manager is responsible for this.

2.7 Data Protection Impact Assessments

NYFRS has adopted a Data Protection Impact Assessment (DPIA) template. Consideration for the completion of a DPIA is a mandatory feature of the procurement process and project framework. DPIAs are carried out prior to any type of processing that is likely to result in a high risk to the individual's interests or any new project that involves the use of personal data. DPIAs are signed off by the Project Lead, DPO and SIRO.

DPIAs are tracked and recorded by sharepoint and being added to the asset register.

DPIAs are referenced in the asset register and the CAO Manager is responsible for maintaining a record of DPIAs and ensuring that reviews occur.

Retrospective DPIA's are not being completed for activities that were originally undertaken pre-GDPR.

2.8 Contracts

NYFRS has a contracts register that identifies all data processing arrangements. A suitable officer (CAO Performance Team Leader) has been identified for maintaining the register. NYFRS has 33 contracts with data processors.

NYFRS has checked all these contracts with data processors to ensure they cover the UK GDPR Article 28 clauses.

Requirements to comply with Subject Access Requests and FOI/EIR requests have been documented in the contractual agreement.

New and renewed contracts are being checked to ensure Article 28 Clauses are covered. After discussion with NYFRS it would be the DPO's recommendation that NYFRS looks at reviewing these contracts.

The Head of Assets is the responsible officer for completing contract checks.

2.9 Information Sharing

NYFRS has policies which clearly document who has the authority to make decisions about regular sharing or one-off disclosures. All sharing decisions including ad-hoc data sharing are documented. All Data Controller sharing agreements have been identified on the Information Asset Register.

NYFRS has worked to restrict shared data sets to what has been agreed.

Statements of compliance have been signed by senior management of both organisations committing them to the terms of these agreements. The agreements include assurances that recipients of that data will delete, destroy or return the data when the purpose is finished or the retention expires.

2.10 Lawful Basis for Processing Personal Data

An information mapping exercise has been completed to identify the various types of processing being carried out.

NYFRS has stated that they have determined the lawful basis for processing personal data and special categories of personal data. However, these have not been included in the IAR so Veritau have been unable to review them. In meeting with the NYFRS contacts it was discussed that NYFRS may need to confirm that it has an appropriate Schedule One condition when processing special category data.

The lawful bases are not explicit on relevant privacy notices.

NYFRS also processes some criminal offence data, a lawful basis for this processing has been determined.

NYFRS has used legitimate interests lawful basis for some processing. NYFRS has stated they have completed adequate legitimate interests tests, but were unable to provide an example so this has not been reviewed by Veritau.

2.11 Consent

NYFRS uses the lawful basis of consent for processing some personal data. This includes:

- Communications
- Photographs to be used on social media or website
- Personal views or statements to be used on social media or website

Records are kept of how and when consent was obtained from individuals.

NYFRS has not yet needed a list of those who have withdrawn consent, as no one has withdrawn consent as of yet. However NYFRS understands the need to maintain a list of withdrawn consent if such a situation occurs.

Consent is freely given and opt-in based.

Individuals are informed of how long consent lasts.

Individuals are informed of how to withdraw consent.

Where consent has expired, data subjects are removed from the list.

2.12 Children's Online Services

NYFRS does not offer online services to children 13 and under.

2.13 Direct Marketing

NYFRS does not carry out direct marketing for the purposes of UK GDPR/PECR.

2.14 Data Subject Rights

NYFRS has an adequate process in place for when an individual exercises their data protection rights (e.g. Subject Access Request, rectification request, etc.).

There is a log in place to record these requests. The log does includes most necessary elements, but doesn't include a column for applied exemptions/reasons for redactions.

NYFRS does have a specific person or team responsible for managing the request.

Guidance has been provided to staff on how to recognise a Data Subject Rights Request. Requests are always acknowledged with a date of expected response. The identities of applicants are adequately verified and the process is detailed in the appropriate policy. The record that have been searched when completing a data subject rights requests are documented. Extensions on complex (including voluminous) SARs are recorded, this is communicated to the applicant.

Where personal data has been disclosed to a third party this is recorded on the data subject's file/case.

When responding to a data subject who has exercised a right, the response includes what was searched, if exemptions were applied. If a request is refused the reasoning is recorded. There is an appeals process.

In the last 12 months NYFRS has had 15 SARs, 53 other data rights requests and 0 reviews requested.

2.15 Records Management

There are formal filing/records management systems for both electronic and hard copy records. When creating new records there is a process in place to ensure those records have appropriate identification, classification, description and formats applied. NYFRS does conduct data quality checks or otherwise ensure data accuracy (e.g. asking data subjects to verify personal data).

NYFRS has a retention schedule which is predominately adhered to. NYFRS has a records disposal register (also known as a destruction log) in place. Confidential waste is adequately disposed of.

There is however a backlog of files held beyond their retention period.

Data processors are adhering to NYFRS's retention schedule. NYFRS have plans to conduct a compliance audit and request confirmation of compliance from data processors.

2.16 Training

NYFRS has a data protection and information security training package. The training is adequately recorded. The training is mandatory. There are different levels of training for different staff members. Staff do refresher training every two years or whenever they undergo a role change requiring a higher level of training. 68% of employees have completed the training, the SIRO is aware that 42% need to complete training, many of these will have had training before and need refresher training.

NYFRS conducts the following role specific training: SIRO, Information Asset Owner, SPOC, Other.

This training is conducted by a range of organisations including Aristi and Act Now. Other training would be sourced if required.

As part of the induction process new starters complete E-Learning and policy reading. Temporary staff are given the same training as permanent staff. There are not necessarily checks in place to ensure that contracted processor staff complete data protection training.

2.17 Security of Personal Data

There is a mobile / remote working policy in place. There are adequate measures in place to mitigate against devices being lost or stolen. Encryption is placed on devices to prevent unauthorised access. Where staff are working remotely security measures are in place.

Info Security and Data Handling Policies are used to prevent data being stored on private devices. This is adequate.

All hardware assets have been identified and documented. Periodic checks are conducted against the hardware asset register. Procedures are in place to ensure the removable media (e.g. USB sticks) are documented. Ports have not been disabled on devices to prevent the use of non-approved removable media. Procedures are in place to ensure all employees and third party users return hardware. All devices are disposed of securely when no longer required.

Measures are in place to ensure that only authorised users access systems and devices. Allocation of privileged access rights are restricted, approved and controlled. User Access rights are reviewed annually. Access rights for temporary staff are restricted, controlled, and removed within an adequate timeframe. Access rights are reviewed if a member of staff moves post. Access rights are revoked upon termination of contract. Access to systems is done using the principle of 'least privilege'. Password rules are set-in policy documents.

Users change passwords periodically and are prevented from using the same password twice.

NYFRS' relevant systems have up-to-date anti-virus. Event logs are not maintained that show user activities and security events.

NYFRS has back-ups which are held off-site at other locations or in the Azure cloud offering. Back-ups are taken daily, weekly and monthly, and have been tested to ensure they are functioning correctly. Overall the back-up arrangements are adequate. NYFRS ensures that data processors use and implement appropriate technical and organisational measures through contractual arrangements.

Agreements and supporting procedures are in place for how data will be shared. Data is encrypted when in transit electronically. When emailing personal data as attachments documents are password protected. Hard copies of personal data being transferred have appropriate measures in place to ensure security.

NYFRS has a business continuity and disaster recovery plan which has been communicated to staff. The plans have been tested and updated, they were recently tested due to the Covid Pandemic situation.

Systems or areas that contain sensitive information are protected to ensure only appropriate personnel can gain physical access. Physical access rights (e.g. passes) are reviewed regularly. There is an adequate clear desk policy. NYFRS does not conduct desk sweeps or other checks to ensure issues are identified, however "watch audits" will look at this. NYFRS aims to position screens away from windows or casual view. Devices are locked when the users are away or the devices are not in use. Access to physical records is controlled and regularly reviewed. Personal data displayed on walls and noticeboards is outside the view of casual observers.

2.18 Information Security Incidents

NYFRS has an adequate policy or process for reporting information security incidents. There is a security incident log in place. In the last year 0 incidents were reported. In future if a reportable incident occurs, it will need to be reported within 72 hours.

Security Incident are investigated. The CAO Manager and the Head of IT are responsible for ensuring these investigations are conducted. Investigations are signed off by the SIRO. These investigations include lessons learned and new controls are implemented as a result. Staff are aware of what to do in the event of a security incident.

2.19 Surveillance

NYFRS operates some overt surveillance. NYFRS has ensured it follows the surveillance code of practice. It has used the Surveillance Commissioner's self-assessment tool on surveillance systems. NYFRS has got an adequate surveillance policy, though as per the earlier section and recommendations, this needs updating. This covers all surveillance systems in operation. NYFRS has not got a standard review checklist for surveillance. There are completed impact assessments for the surveillance system. There is signage for the CCTV. The camera angles are adequate for purpose and don't infringe on private property or public paths. Retention periods for surveillance data has been determined. Disclosures to third parties such as police are adequately recorded.

3) 2020-2021 Summary of Recommendations

Area of Report	Action	Additional Information
ICO Registration		
Governance and Accountability	1) Create Information Governance Framework and strategy documents.	1) The framework is there to ensure clear lines are drawn as to what policies are relevant to information governance, so these policies can be provided to the ICO upon request, are properly updated and so they don't get "lost". Frameworks are a great way to have a very high level understanding of what policies the organisation has. Strategy documents exist so that the organisation has a clear understanding of what its short and long term goals are in terms of information governance/data protection compliance. Veritau can provide examples if necessary.
Information Governance Policies	2) CCTV Scheme – Retention of Recorded Images section should	

	aim to be more specific in timeframe. The policy says copies should be reviewed annually, but most organisations set a date of one-two months if there's no ongoing investigation. This therefore seems a little long. I understand what NYFRS intends with the loop, but NYFRS should aim to be more specific with how long that loop takes. It seems like this may be 72 hours from the appendix documentation, but the PN says 49 days. It is much preferable to set an amount of days wherever possible. 3) CCTV Scheme - Subject Access Requests – out of date information. 4) FOI and EIR Policy – 5.5 – made via the website – this link no longer works.	3) (See your Data Subject Rights Request Procedure – you either want to bring this into line with that or direct people to it).

	5) Records Management Policy – Duties – Senior Information Risk Owner - needs updating. 6) Special Category Data Policy – this need to be adopted. 7) Information Security and Handling Policy – The review dates on the front page have not been updated.	6) Required to properly use the full suite of Article 9 lawful basis.
Privacy Notices	8) CCTV –retention period issue as above. 9) Privacy Notices general – agree matching format across the notices and include DPO details.	9) Matching formats seem a minor issue, but they help us spot issues and look thought-out upon ICO inspection.
Websites, Social Media and Cookies	10) Recommend putting a link to the Website and Social Media Privacy Notice on the 'about' section of the Facebook page.	
Information Asset Management	11) Recommendations to meet minimum ROPA requirements:	11-12) Further information on each of these is included in the report above. However it is important to

	The "Purpose" of the asset, and the "description" are mandatory fields. The NYFRS asset register does have these fields, but they would benefit from enhancement. Include a "details of transfers to third countries" section. If NYFRS doesn't transfer any personal data to third countries I would recommend that a column is still added to make this clear. Include a description of the technical and organisational security measures. Recommendations to meet best practice as defined by the ICO: The ROPA should document the lawful basis (Article 6 and Article 9 Conditions of the UK GDPR) Where consent is used, the ROPA should document how consent is sought and where evidence of consent is kept. The ROPA should include a column to record any personal data breaches affecting an asset.	state that the Information Asset Register fulfils the obligations of a ROPA and should therefore be an accurate, up-to-date document that can be supplied to the ICO upon request, with minimal edits.

	The asset should include a retention period or identify where the retention periods can be found. 12) The Information Asset Register needs to be kept up to date.	
Data Protection Impact Assessments	13) NYFRS should start the process of doing retrospective DPIAs.	13) Retrospective DPIAs weren't and aren't an obligation under GDPR. However, they can identify weaknesses and gaps, are considered best practice and if a particularly serious DP concern or breach is reported to the Commissioner they may take a much better view of the organisation if the organisation has accurately considered risks and can demonstrate privacy by design. NYFRS should use a risk-based approach when completing retrospective DPIAs, selecting high-risk processes first.
Contracts	14) Review data processing agreements.	14) All contracts were reviewed for GDPR, however after three years

		and with a lot more internal knowledge and access to external knowledge in the form of Veritau, it would be beneficial to review the data processing agreements.
Information Sharing		
Lawful Basis for Processing Personal Data	15) Review information assets and identify where Schedule One condition is required. 16) Notices should be reviewed to explicitly include what legal basis NYFRS is relying on.	
Consent		
Children's Online Services		
Direct Marketing		
Data Subject Rights		
Records Management	17) There is a backlog of physical files past retention period to be destroyed.	17) Veritau were informed and a plan is in place to deal with this.
Training	18) NYFRS need to improve number of employees who have completed relevant training.	18) When reporting a data breach to the ICO, the ICO does not ask whether someone has done training, the ICO asks whether someone has completed training in the last two years. Therefore to the regulator,

	19) Data Processor Agreements, procurement and other means should be used to ensure contracted processor staff have completed data protection training.	having regular refresher training is very important.
Security of Personal Data	20) Check whether systems have Event Log functionality.	20) Event logs, also called audit logs, are a great tool especially in the rare event of S170 breaches. Often systems have this functionality built in and it is simply not turned on or unknown to staff. Where it is missing, it may be a good idea to keep a note of that and look at that the next time there is a procurement/tendering exercise or the supplier asks for development feedback.

	21) NYFRS should look at disabling ports to prevent the use of non-approved removable media.	21) NYFRS did inform me that this is something ICT has previously looked at, but no capacity in staff was available, so no requests for funding were made. In light of the renewed focus on Data Protection following GDPR and the ever-growing increased risk of cyber-attacks, I would recommend that this is considered again.
Information Security Incidents		
Surveillance	22) Should draft a standard checklist and review CCTV.	