Compliance Audit Data Sheet

Data Protection Compliance Audits

Aims of data protection compliance audits

DPP's compliance audits go beyond the basic requirements of data security and address wider aspects of data protection including:

- Mechanisms for ensuring that information is obtained and processed fairly, lawfully and transparently;
- Data quality assurance - ensuring that information is accurate, complete and up-to-date, adequate, relevant and not excessive;
- Data minimization – ensuring that a minimum of data is collected and not retained any longer than is necessary;
- Documentation on authorised use of systems, e.g. codes of practice, guidelines etc.;
- Compliance with individual's rights, such as subject access requests;
- Compliance with the data protection legislation in the context of other pieces of legislation such as the Privacy and Electronic Communications Regulations.

Why should organisations audit?

The key reasons for carrying out data protection audit activities are:

- To assess the level of compliance with the Data Protection Act 2018/GDPR;
- To assess the level of compliance with the organisation's own data protection system/arrangements;
- To identify potential gaps and weaknesses in the data protection system/ arrangements;
- To provide information for an on-going, monitoring and review of the data protection system and the management of data processing operations review;
- To check that sufficient evidence is accumulating of compliance for accountability purposes.

Audit objectives

When carrying out a data protection audit for an organisation DPP will look

- To verify that there is a formal (i.e. documented and up-to-date) data protection system in place.
- To verify that all the staff in the area involved in data protection:
  - Are aware of the existence of the data protection system
  - Understand the data protection system
  - Use the data protection system
- To verify that the data protection system in the area actually works and is effective.

Audit benefits

Organisations who undertake a compliance audit can expect to achieve a number of benefits including:

- Facilitates compliance with the Data Protection Act;
- Measures and helps improve compliance with the organisation's data protection system;
- Increases the level of data protection awareness among management and staff;
- Provides information for data protection system review;
- Improves customer satisfaction by reducing the likelihood of errors leading to a complaint.

Audit delivery

Audit Planning

DPP will agree the audit scope with the client including:

- Whether it is an adequacy audit, a compliance audit or a combination of the two;
- A list of the data protection functions to be reviewed (e.g. data subject rights, compliance with the data protection principles, supply chain review, breach handling processes etc.);
- A list of the data processing activities to be reviewed (e.g. marketing and sales order processing, use of social media);
- A list of the departments to be reviewed (e.g. HR, operations, sales, marketing, clinical care etc.).

Adequacy audit

DPP require the following information from the client prior to undertaking the adequacy audit.

- Details of the data protection lead/compliance officer;
- A copy of all of the documents forming the information governance framework (i.e. all policies, procedures, work instructions, guidance etc. relating to data protection, handling personal data, using information system information security etc.);
- Article 30 records or a written statement of exemption. Where an organisation is exempt from maintaining records of processing activities on the Article 30 it is required to provide DPP with the following:
    - An information asset register or list of data processing systems;
    - A list of the purposes for which personal data are processed (including the types of personal data, categories of data subject, and lawful basis for processing);
      A list of third parties to whom the organization discloses personal data (including data processors).

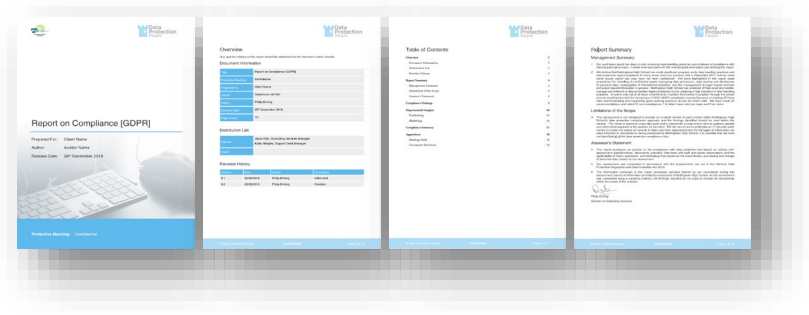
Compliance audit

DPP require the following information from the client prior to undertaking a compliance audit.

- Details of the data protection lead/compliance officer;
- A list of the databases/systems and filing systems containing personal data or information asset register;
- An organisation chart showing departments and their roles;
- A list of data protection policies implemented by the organisation;
- A copy of the data protection policy;
- A copy of the information security policy;
- A copy of the privacy policies in use;
- A copy of the data retention schedule;
- A list of data processors and data sharing agreements;
- Article 30 records or a written statement of exemption. Where an organisation is exempt from maintaining records of processing activities on the Article 30 it is required to provide DPP with the following:
    - An information asset register or list of data processing systems;
    - A list of the purposes for which personal data are processed (including the types of personal data, categories of data subject, and lawful basis for processing);
    - A list of third parties to whom the organization discloses personal data (including data processors).

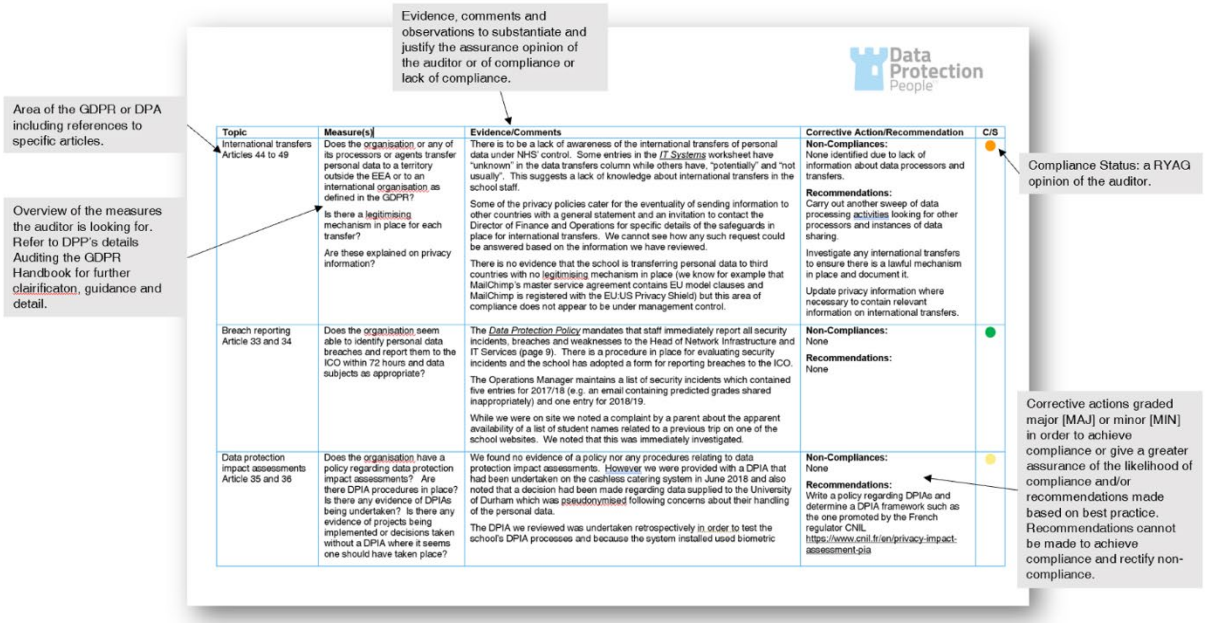
Audit report

The audit report will be presented using the following structure



- Front cover
- Overview
- Table of Contents
- Report Summary containing an overview of the report findings and the auditor's statement.

- Compliance Findings containing:
    - A list of topical areas in the GDPR and a reference to specific articles;
    - A summary of the measures the auditor is looking for and/or testing the organisation against in order to evaluate the likelihood of compliance;
    - Evidence, comments and observations made or used by the auditor to substantiate their opinion of compliance rating;
    - Corrective actions rated as either major or minor non-compliances where the organisation is thought not to comply with the requirements of the law, or recommendations where the auditor cannot obtain sufficient evidence to form an opinion or where an observation is not strictly a non-compliance but where compliance could be improved upon with the adoption of best or good practice;
    - Compliance status graded red, amber, yellow, or green based on the evidence presented.
    - any specific insights derived from particular areas of the organisation or specific departments (e.g. observations in the marketing or HR department based on detailed interviews (see below).
- a compliance summary of the non-compliances and recommendations
- Report recommendations RAG rated: -
    - High Assurance - 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 noncompliance with the DPA.
    - Reasonable Assurance - 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 noncompliance with the DPA.
    - Limited Assurance - 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 noncompliance with the DPA.
    - Very Limited Assurance - 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.
- appendices comprising a list of interviewees and documentation reviewed.



Topic	Measure(s)	Evidence/Comments	Corrective Action/Recommendation	C/S
International transfers Articles 44 to 49	Does the organisation or any of its processors or agents transfer personal data to a territory outside the EEA or to an international organisation as defined in the GDPR? Is there a legitimising mechanism in place for each transfer? Are these explained on privacy information?	There is to be a lack of awareness of the international transfers of personal data under NHS' control. Some entries in the *IT Systems* worksheet have "unknown" in the data transfers column while others have, "potentially" and "not usually". This suggests a lack of knowledge about international transfers in the school staff. Some of the privacy policies cater for the eventuality of sending information to other countries with a general statement and an invitation to contact the Director of Finance and Operations for specific details of the safeguards in place for international transfers. We cannot see how any such request could be answered based on the information we have reviewed. There is no evidence that the school is transferring personal data to third countries with no legitimising mechanism in place (we know for example that MailChimp's master service agreement contains EU model clauses and MailChimp is registered with the EU-US Privacy Shield) but this area of compliance does not appear to be under management control.	**Non-Compliances:** None identified due to lack of information about data processors and transfers. **Recommendations:** Carry out another sweep of data processing activities looking for other processors and instances of data sharing. Investigate any international transfers to ensure there is a lawful mechanism in place and document it. Update privacy information where necessary to contain relevant information on international transfers.	
Breach reporting Article 33 and 34	Does the organisation seem able to identify personal data breaches and report them to the ICO within 72 hours and data subjects as appropriate?	The *Data Protection Policy* mandates that staff immediately report all security incidents, breaches and weaknesses to the Head of Network Infrastructure and IT Services (page 9). There is a procedure in place for evaluating security incidents and the school has adopted a form for reporting breaches to the ICO. The Operations Manager maintains a list of security incidents which contained five entries for 2017/18 (e.g. an email containing predicted grades shared inappropriately) and one entry for 2018/19. While we were on site we noted a complaint by a parent about the apparent availability of a list of student names related to a previous trip on one of the school websites. We noted that this was immediately investigated.	**Non-Compliances:** None **Recommendations:** None	
Data protection impact assessments Article 35 and 36	Does the organisation have a policy regarding data protection impact assessments? Are there DPIA procedures in place? Is there any evidence of DPIAs being undertaken? Is there any evidence of projects being implemented or decisions taken without a DPIA where it seems one should have taken place?	We found no evidence of a policy nor any procedures relating to data protection impact assessments. However we were provided with a DPIA that had been undertaken on the cashless catering system in June 2018 and also noted that a decision had been made regarding data supplied to the University of Durham which was pseudonymised following concerns about their handling of the personal data. The DPIA we reviewed was undertaken retrospectively in order to test the school's DPIA processes and because the system installed used biometric	**Non-Compliances:** None **Recommendations:** Write a policy regarding DPIAs and determine a DPIA framework such as the one promoted by the French regulator CNIL https://www.cnil.fr/en/privacy-impact-assessment-pia	