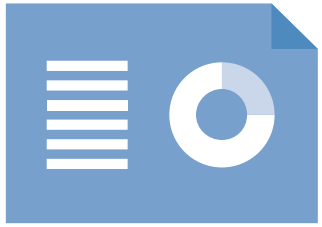
The University of Warwick

Data Protection Audit Report

March 2020

Information Commissioner's Office

Executive summary



Audit Methodology

The Information Commissioner is responsible for enforcing and promoting compliance with the General Data Protection Regulation (GDPR), the Data Protection Act 2018 (DPA18) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

The ICO approached the University of Warwick in October 2019 to offer a consensual audit. The University agreed to participate in the audit and ICO auditors visited the University in January of 2020.

The purpose of the audit is to provide the Information Commissioner and the University of Warwick with an independent assurance of the extent to which the University, within the scope of this agreed audit, is complying with data protection legislation.

It was agreed that the audit would focus on the following area(s):

Scope Area	Description
Governance & Accountability	The extent to which information governance accountability, policies and procedures, performance measurement controls, and reporting mechanisms to monitor data protection compliance to both the GDPR and national data protection legislation are in place and in operation throughout the organisation.
Security of Personal Data	The extent to which there are appropriate technical and organisational measures in place to ensure the confidentiality, integrity and availability of manually and electronically processed personal data.
Training & Awareness	The provision and monitoring of staff data protection, records management and information security training and the awareness of data protection regulation requirements relating to their roles and responsibilities.

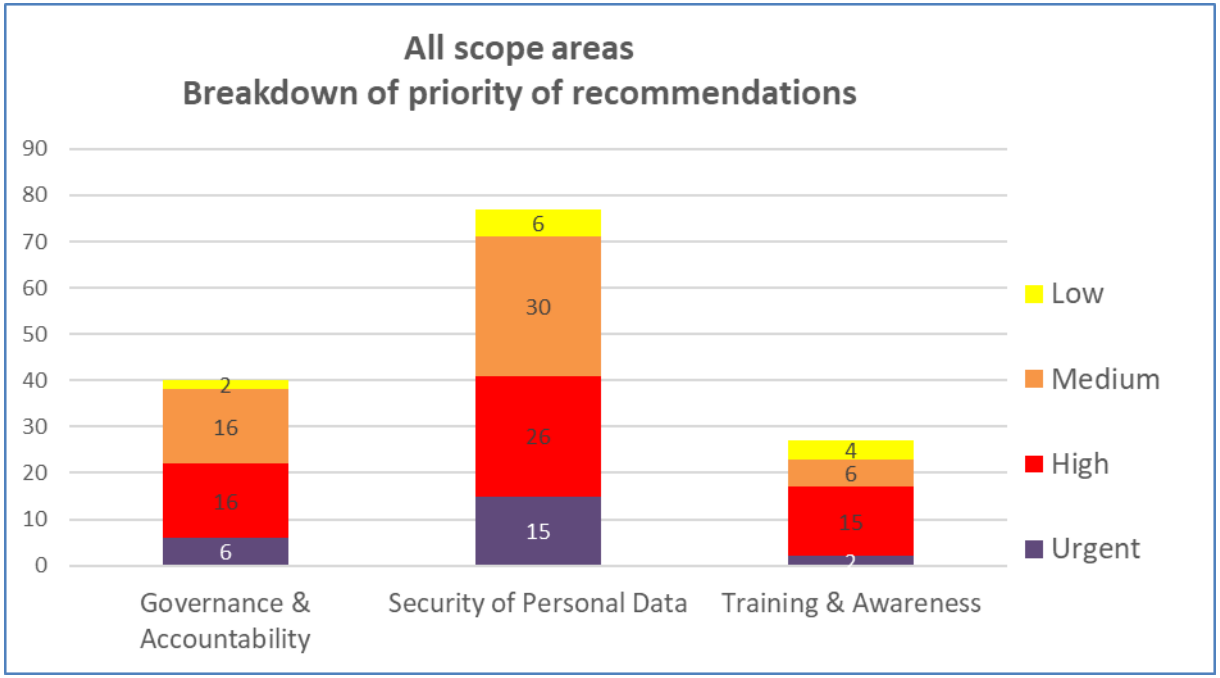
The audit was conducted following the Information Commissioner's data protection audit methodology. The key elements of this are a desk-based review of selected policies and procedures, on-site visits including interviews with selected staff, and an inspection of selected records.

Where weaknesses were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist the University of Warwick in implementing the recommendations each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. the University of Warwick's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

Audit Summary

Audit Scope Area	Assurance Rating	Overall opinion
Governance & Accountability	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.
Security of Personal Data	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.
Training & Awareness	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.

Priority Recommendations



Areas for Improvement

Cross-scope:

- The current policy framework is not being effectively managed. A significant number of policies are out of date, in draft, or not in place and there is a lack of consistency across documents. There is no sign off, authorisation or review process and there is often no enforcement of those policies or any assurance of compliance particularly at departmental level. A clear, consistent and regularly reviewed policy framework is essential and underpins data protection compliance and assurance.

- There is a data protection oversight body (the Data Protection and Privacy Group – DPPG) in place but there are concerns that it is not functioning effectively as meetings are regularly cancelled, it lacks focus and is not being used as a forum to provide consistent management to long term data protection concerns or to immediate pressing issues.

Governance & Accountability:

- Whilst there is a governance framework in place at the University it does not provide adequate support to the Information Governance (IG) and Records Management agendas. The University needs to review its overall governance approach to IG to ensure that the Board drives and supports compliance.

- Key Performance Indicators (KPIs) to measure IG compliance are not set.

- There is no formal Data Protection Impact Assessment (DPIA) process in place, or formal DPIA policy and procedure.

Security of Personal Data:

- A number of technical vulnerabilities have been highlighted in the report and communicated separately to the University's executive function. These should be acted on as a priority.

- The University is not practising wireless network segregation.

- The University does not have a strategic lead for all aspects of information security covering the whole organisation.

- The University is lacking centralised oversight of information security processes, control and potential risk at departmental level.

- The University does not have coordinated and in depth information and control over hardware and software assets or a clear process of ownership of those assets. There is a mixed estate of end user devices, servers, and wide variation in the security controls in place on the devices, the applications they host and the personal data resident on those systems.

- There is a lack of oversight and control over data from certain core systems feeding into other information resources risking unanticipated data leakage.

- There is no separation between student and staff email address directories, raising the risk of information being sent to a student incorrectly.

- The University does not undertake coordinated actions in response to persistent security issues, for example having continuous monitoring at DPPG, detailing an action plan with cross departmental procedures and

swift drafting and deployment of policy reinforced by training and awareness.

Training & Awareness

- The University has not mandated its IG training activities across departments.
- There is no effective central oversight of completion rates and the University has no effective processes in place to ensure completion by all staff.
- Specialised data protection training is missing across University departments where data processing activities are directly affected by the GDPR.
- University staff involved in data breaches are not given additional training.

Disclaimer

The matters arising in this report are only those that came to our attention during the course of the audit and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rest with the management of the University of Warwick.

We take all reasonable care to ensure that our audit report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.

This report is an exception report and is solely for the use of the University of Warwick. The scope areas and controls covered by the audit have been tailored to the University of Warwick and, as a result, the audit report is not intended to be used in comparison with other ICO audit reports.