Scottish Government Data Protection Officer Job Description

Overview

The Data Protection Officer (DPO) will be expected to help shape the Scottish Government's approach to the implementation of the new General Data Protection Regulation (GDPR), which will come into effect in May 2018.

This post sits within the Directorate for Internal Audit. The post-holder will have a key assurance, compliance and advisory function on data protection matters, from assisting business areas in Scottish Government with carrying out data protection impact assessments to leading a programme of audits of personal data processing activities, and reporting key findings and recommendations to the Executive Team. The post holder will need to engage with a range of senior stakeholders both internally and externally including the Information Commissioner's Office.

The DPO will also be the point of contact with the regulator (the UK Information Commissioner's Office) and with members of the public. You will work collaboratively with the team who are responsible for providing advice and guidance on data protection and colleagues in information security, legal and records management.

Main Duties

Monitor compliance with data protection legislation, including the assignment of responsibilities, awareness-raising including overseeing training of staff involved in processing operations.

Provide leadership in raising the profile of data protection compliance with those staff responsible for managing projects or work-streams that involve the processing of personal data - this will involve close working with colleagues across the organisation.

Maintain relevant registrations with the Information Commissioner's Office.

Engagement with the Information Commissioner.

Design and implement a planned programme of risk based audits to test compliance, and report key findings and recommendations to the Executive Team.

Provide advice to Information Asset Owners following both data processing audits and data breaches, monitoring and working with the business to address identified issues.

Liaise with the Information Commissioner's Office by acting as the contact point on and provide information as requested on SG compliance in this area.

Ensure continuing professional development by regularly self-assessing training needs and taking steps to ensure any needs identified are met.

Essential Criteria

1. A good knowledge and understanding of data protection laws and practices including the DPA and GDPR and an understanding of the impact of the legislative changes.
2. Demonstrable experience of building relationships at senior levels within the organisation, both supporting but also challenging senior stakeholders.
3. Strong analytical skills, including the ability to convey analytical information effectively to senior audiences, both written and orally.
4. A good understanding of information security and the relationship between this and data protection.