Data Protection Officer (DPO) Responsibilities

The Commission's Data Protection Officer (DPO) is the Director of Governace. The DPO is responsible for the Commission's compliance with the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) including the Law Enforcement Directive (LED). The role of the DPO covers all data processing activities. **As the DPO, the Head of Governance will, in accordance with Article 39 of the UK GDPR and Data Protection Act Part 3 Section 71:**
1. Inform and advise the Commission, any third-party processor engaged by the Commission and employees, about their obligations to comply with the UK GDPR and other data protection legislation;
2. Provide advice on the carrying out of Data Protection Impact Assessments under section 64 of the LED and Article 35 of the UK GDPR and monitor compliance with that section;
3. Provide the Commission with updates to any changes in legislation;
4. Raise awareness of data protection issues;
5. Provide training to staff involved in data processing;
6. Conduct internal audits to ensure compliance and address potential issues proactively;
7. Act as the point of contact for the ICO on issues relating to processing, including in relation to the consultation mentioned in section 65 (LED) and Article 36 of the UK GDPR and consulting with the Commissioner, where appropriate, in relation to any other matter;
8. Act as the point of contact between the Commission and other Data Protection Supervisory Authorities
9. Act as the point of contact for people whose personal information is being processed (employees, clients etc) in accordance with Article 38 of the UK GDPR.
10. Co-operate with the ICO
11. Monitor compliance with Commission policies in relation to the protection of personal data including: i. assigning responsibilities under those policies ii. raising awareness of those policies iii. training staff involved in processing operations, and iv. conducting audits required under those policies.
12. Provide risk-based advice to the organisation in relation to data protection and GDPR.
13. The SIRO and/or the DPO must approve any procurement involving personal and/or commercially sensitive information. The SIRO and/or the DPO has the authority to raise a formal concern with the Accounting Officer regarding a procurement (or information sharing arrangement etc) that contravenes the organisation's core information security and information governance policies.

Policy Responsibilities

Responsible for:
Corporate Governance Framework: Corporate Governance Framework
Speak Up (whistleblowing) Policy: Corporate Governance Framework - Appendix 4 – Speak Up (Whistleblowing) policy
Complaints Policy: Corporate Governance Framework - Appendix 5 – Complaints policy
Code of Conduct for Commissioners: Corporate Governance Framework - Appendix 8 – Code of conduct for Commissioners
Managing Conflicts of interest policy: Gambling Commission: Managing conflicts of interest policy
Gifts and Hospitality Policy Freedom of Information Policy Data Protection Policy Information Classification Records Retention Schedule Records Management policy Clear desk guidance Information Management Handbook Risk Management Risk Appetite statement Vetting Internal Governance Framework
Would also have a role in relation to the employee Code of Conduct: Corporate Governance Framework - Code of conduct for employees
Regulatory Panel guidance: Regulatory decisions: Procedures and guidance for regulatory hearings
Contract owner for: • Internal audit (currently supplied by GIAA) • Risk management software • Board portal software • Information request software • Board Effectiveness Review (external review to be carried out in Q4)
Responsible for terms of reference for Board Committees, ExCo and ExCo subcommittees and ensuring various things are published on the website (decs of interest, Commissioner bios, minutes of board/expert groups, gifts and hospitality and Chair/CEO engagements).