Data Protection Officer Responsibilities

Named Contact for Data Subject Complaints

Single point of contact for the regulator (ICO)

Oversight & Approval of:

- Advice & Guidance
- Records of Processing Activity
- Compliance Reporting
- Performance Auditing
- Security Incidents
- Impact Assessments
- Risk Management
- Information Sharing
- Statutory Requests
- Complaints (Direct & ICO)
- Policy
- Training
- Registration

igs | Essex County Council

Named Contact for Data Subject Complaints

The DPO's name and work contact details should be published in order for Data Subjects to direct their enquiries and complaints

Single point of contact for the regulator (ICO)

Where there is involvement with the ICO, the DPO should act as the single point of contact to ensure that correspondence is well managed, approved and within timescales

Oversight & Approval of:

Advice & Guidance:

The DPO should be sufficiently knowledgeable in Data Protection law to provide correct guidance on the legal requirements of processing personal data to employees and data processors for which the organisation is responsible

Records of Processing Activity:

The DPO should be monitoring the process of reviewing the Organisation's Records of Processing Activity, which documents compliance with the Data Protection Act, in order to approve its completeness, currency and accuracy

Compliance Reporting:

The DPO should be satisfied with the scope of reporting on Data Protection compliance metrics, its frequency, its accuracy, and that the receiving audience is appropriate and gives the report sufficient weight. The DPO should provide commentary on reports so that senior leaders can receive qualified opinion on whether the Organisation is compliant

Performance Auditing:

The DPO should be satisfied that there is appropriate testing of the Organisation's compliance activities, its frequency and that there is either a satisfactory outcome or that action points are identified as part of improvement plans to which senior leaders give sufficient support.

Security Incidents:

The DPO should be assured that security incidents are being correctly identified, reported, investigated and recorded effectively. The DPO should advise the Organisation on whether a particular incident meets the criteria for reporting to the ICO, and with the SIRO's agreement, managing the ICO reporting process within the statutory timescale.

Impact Assessments:

The DPO should ensure that where activities which require a statutory Data Protection Impact Assessment, this is undertaken. Where an assessment is undertaken, the DPO must be the role to approve that the proposed processing of personal data is compliant with the law.

Risk Management:

The DPO should monitor the Organisation's risk review process to ensure those risks which impact on Data Protection compliance are appropriately reviewed and the DPO has the opportunity to comment on and approve the identified mitigations.

Information Sharing:

The DPO should ensure that employees have clear guidelines to follow on when it is appropriate to share personal data and how this should be done securely. Where new requirements to regularly share data are identified, the DPO should arrange for Information Sharing Protocols to be approved before the activity commences.

Statutory Requests:

The DPO should be satisfied that the Organisation has in place effective processes for recognising considering and responding to statutory requests relating to the Data Subject rights under Data Protection law.

Complaints:

The DPO should be satisfied that the Organisation has in place effective processes to identify and manage complaints made regarding the processing of personal data from both members of the public and the ICO.

Policy:

The DPO should ensure that all policies which relate to the processing of personal data are legally compliant, reviewed at an appropriate frequency, approved with DPO guidance by senior leaders, and that they are accessible to appropriate audiences.

Training:

The DPO should be satisfied that employees receive appropriate training in the Organisation's data processing policies and procedures according to their roles and responsibilities. Relevant training activities and awareness communications should be recorded and approved by the DPO.

Registration:

The DPO should be satisfied that there is an effective process in place for registering the Organisation's details with the ICO, reviewing this annually, paying the annual fee to the ICO and renewing when the registration expires.