Accountability at the ICO

As part of our preparations for the requirements of GDPR, we have reviewed how we demonstrate accountability for our processing activities.

The Information Commissioner's Office (ICO) is a public authority and therefore we have appointed a Data Protection Officer (DPO) in compliance with Article 37 of the General Data Protection Regulation.

Our Data Protection Officer plays a key role in ensuring our accountability, but is not solely responsible.

We have a Privacy and Information Management Framework. This is a network which enables us to embed cultural and systematic good practice, identify and manage our information risks, and monitor compliance.

These are the key roles:

Senior Information Risk Owner – Paul Arnold, Deputy Chief Executive Officer
Data Protection Officer – Louise Byers, Head of Risk and Governance
Senior Information Asset Owners – James Dipple-Johnstone, Deputy Commissioner (Operations), Steve Wood, Deputy Commissioner (Policy), Emma Bate, General Legal Counsel
Information Asset Owners – all Heads of Department
Local Information Management Officers – nominated by IAOs, number dependent on volume and nature of processing of information
Local Asset Administrators – nominated by IAOs, number dependent on volume and nature of processing of information

Our SIRO, DPO and IAOs are responsible for making sure that our business processes and decision making are in line with GDPR requirements and good practice.

We also have central information governance teams who provide advice, monitor compliance and carry out key tasks like responding to requests, handling security incidents, assist in managing records and promote good privacy, security and information management practices.

Our approach has 'privacy by design and default' at the forefront. We have an established privacy assessment process led by our Data Protection Officer who is available to provide advice throughout the process. This process is linked to our procurement, supplier assessment and contract management processes.

We have key accountability documentation including a record of our processing activities, corporate retention schedule and information asset register. Our business processes require that decisions and rationale are documented.

We are committed to being transparent with people who interact with us and use our services. Required changes to our privacy notice are identified and implemented through our privacy assessment and procurement processes.

Training in data protection and governance for new starters and existing staff is ongoing. Where specific training needs are identified, we are committed to providing appropriate training and support.

Our Data Protection Officer

This explains how our Data Protection Officer fits into our governance structure.

The Information Commissioner's Office (ICO) is a public authority and therefore we have appointed a Data Protection Officer (DPO) in compliance with Article 37 of the General Data Protection Regulation.

This statement explains how the role of the Data Protection Officer works within the ICO.

Our Data Protection Officer is Louise Byers. Louise is also the Head of Risk and Governance and previously, was the Head of Good Practice since 2010. The main focus of the Good Practice (now named Assurance) department is to conduct data protection compliance audits across a wide range of sectors, sharing good practice and identifying actions to improve information rights practices. Louise has significant experience in data protection and compliance monitoring and is very familiar with the processing activities of the ICO.

Independence

Our DPO is free of conflicting priorities and is able to raise issues in the way and in the forum they see fit, without approval from their line manager or others to do so. Our DPO is not penalised for performing their tasks.

Reporting to highest level of management

The DPO is accountable to the ICO's Management Board, the most senior executive board at the ICO, consisting of the ICO's Senior Leadership Team and Non Executive Directors.

The DPO is responsible for reporting risks or opportunities and recommending appropriate actions in relation to the ICO's processing of personal information. Our Management Boards include our Senior Information Risk Owner (SIRO). Our DPO has very regular contact with all members of our Senior Leadership Team (SLT), including the Information Commissioner, our Audit Committee and with all Heads of Department. SLT is responsible for corporate planning and making business decisions which might impact on how we process personal information. Our Heads of Department implement those plans and decisions.

Our Privacy and Information Management Framework

We have an established Privacy and Information Management Framework which includes specified roles including our DPO.

Resources and access

The Risk and Governance department includes our Information Management, and Information Access teams. Our Head of Cyber Security sits separately but works closely with our DPO. Work to ensure our internal data protection compliance, including completion of Data Protection Impact Assessments, is carried out and monitored by these teams of staff.

The resources of these teams is under regular review and increased or changed where needs are identified.

Our DPO has access to all of our information systems and access to all services and staff if they need input, information or support.

DPO tasks

The requirements of Article 39 are included in the DPO job description.

Our DPO's other tasks

We have appointed an internal, existing employee as our DPO who has existing professional duties. As DPO and Head of Risk and Governance, the tasks and focus of each role complement each other, and do not conflict. Neither responsibility is focused on determining the purposes and means of processing personal data but are both focused on providing advice about the risks, mitigations, safeguards and solutions required to ensure our processing is compliant and supported by our business decisions.

Visibility

Our DPO's contact details are included within our privacy information and records of processing activities. We also include their name and photograph within our internal information governance training, which is completed by all staff. We have a dedicated email address and monitored inbox for data protection queries or complaints received internally or externally.

Our DPO is our contact with the Information Commissioner's Office in its capacity as UK supervisory authority.

Decision making

Where the advice of the DPO is not followed, this is documented.

If you have any queries please email dpo@ico.org.uk.