IfATE
Shaping skills training

Data protection and information governance practitioner

Details of standard

Occupation summary

This occupation is found in organisations of all sizes across all sectors where personal and commercial data is processed. Data protection and information governance practitioners work in varied environments including in an office, onsite, or remotely.

The broad purpose of the occupation is to provide regulatory and technical advice and guidance providing assurance to key stakeholders and regulators of compliance with information governance (IG) and data protection (DP) requirements. Organisations must comply with information governance legislation to protect the confidentiality, integrity and availability of its information assets. The data protection and information governance practitioner (DP&IGP) will contribute to the annual work plan and assist in the planning and organisation of IG, ethics and DP activities. The DP&IGP will also provide advice and training with regard to improving data management and will support the senior team in the development and delivery of operational and strategic information requirements. The role requires work to be undertaken under explicit and legally defined timeframes (for example, data breaches must be reported within 72 hours and Data Subject Access Requests must be fulfilled within one calendar month).

In their daily work, an employee in this occupation interacts with a range of internal stakeholders including members of their own team, other departments such as IT, legal, HR, marketing, senior management and the board of directors. They also interact with external stakeholders such as members of the public, customers, Supervisory Authorities, The Information Commissioner's Office (ICO), technology vendors, academics, industry bodies, external legal departments, human rights organisations, consumer rights organisations and law enforcement.

An employee in this occupation will be responsible for assisting the organisation in its compliance with information governance and data protection best practice and associated laws and regulations. They will oversee and manage the day-to-day coordination of information requests such as data subject rights, freedom of information and environmental information regulations. In addition, they will oversee compliance with Information and Records Management for example the development and maintenance of retention schedules. They assist in the maintenance and administration of the organisations' information and governance framework such as corporate information management, records of processing activity, developing privacy notices, conducting information audits and data breach investigations. On occasion the DP&IGP supports projects through ensuring privacy by design and default. They may also conduct a data protection impact assessment (DPIA) and third-party

supplier due diligence. They analyse data and develop briefings for senior leadership on data protection and information governance controls. They may investigate information governance complaints and incidents from internal or external stakeholders. This role will work on their own and in a range of team settings. They work within agreed budgets and available resources. The DP&IGP work without high levels of supervision, usually reporting to senior stakeholders. They may occasionally be responsible for decision making, but more often will guide or influence the decisions of others.

Typical job titles include:

Data protection lead | **Data protection manager** | **Information compliance officer**

Information governance lead | **Information governance officer** | **Privacy officer**

Occupation duties

DUTY	KSBS
Duty 1 Support senior management by contributing to the development of policies and guidance to ensure the organisation complies with its statutory and regulatory information governance (IG) and data protection (DP) responsibilities.	K1 K6 K7 K8 K11 K12 K16 S1 S2 S3 S7 S9 S13 B1 B2 B5 B6
Duty 2 Work with internal stakeholders to review and maintain retention schedules, providing specialist support, advice and guidance to ensure appropriate disposal of data in compliance with legislation, regulation and good practice.	K1 K7 K11 K16 S1 S4 S7 S9 S12 B1 B2
Duty 3 Develop and deliver in-house IG and DP training and awareness packages for all internal stakeholders such as IT, legal, HR, marketing, senior management and the board of directors.	K1 K5 K6 K7 K9 K10 K11 K12 K13 K14 S2 S3 S7 S9 S13 B1 B2 B3 B4 B5 B6
Duty 4 Co-ordinate and support the organisation's formal and documented record of processing activities in line with legislation, regulation and good practice.	K1 K4 K11 K15 S1 S2 S3 S9 S14 B2 B5 B6
Duty 5 Analyse data and present the outcomes to their key stakeholders on key risk, trend and performance indicators such as training, information requests, data breaches and records management.	K1 K2 K4 K5 K11 K13 K16 S1 S2 S3 S6 S7 S9 S11 S14 B1 B2 B3 B6
Duty 6 Manage, co-ordinate and respond to information requests such as Freedom of Information (FOI), Individual Rights (IR), Environmental Information Regulation (EIR) and Data Protection (DP), within the statutory deadlines.	K1 K3 K5 K7 K8 K9 K10 K11 K12 K14 K15 K16 S1 S2 S3 S4 S5 S6 S7 S8 S9 S12 S13 B1 B2 B3 B5 B6
Duty 7 Undertake or assist in the completion of data protection impact assessments (DPIA) in order to identify and mitigate any potential risks to the organisation and continue to monitor the status of the risk.	K1 K3 K4 K5 K6 K7 K8 K10 K11 K12 K13 K15 K16 S1 S2 S3 S4 S5 S7 S9 S11 S12 S14 B1 B2 B3 B5 B6
Duty 8 Investigate reported personal data breaches providing advice and guidance to the organisation.	K1 K2 K4 K5 K8 K9 K11 K12 K13 S1 S2 S3 S4 S5 S6 S7 S8 S9 S10 S11 S12 S14

Determine the need to escalate, as appropriate, to the Supervisory Authority.	B1 B2 B3 B5 B6
Duty 9 Undertake routine and ad-hoc data protection audit and testing controls for both internal functions and third-party suppliers, producing audit reports for senior managers.	K1 K2 K3 K4 K8 K11 K15 S1 S2 S3 S6 S8 S9 S11 S12 B1 B2 B3 B5 B6
Duty 10 Provide day to day support and specialist advice across the organisation for all matters regarding IG and DP such as compliance with data protection principles.	K1 K3 K4 K5 K6 K7 K8 K10 K11 K12 K13 K14 K16 S2 S7 S8 S9 S13 B1 B2 B3
Duty 11 Contribute to continuous improvement of systems and processes to ensure procedures, policies and guidance are updated in line with technology advancements, legislative and social changes.	K1 K2 K3 K6 K8 K12 K15 K16 S2 S3 S7 S9 S11 S14 B1 B2 B3 B4
Duty 12 Provide support for the completion and submission of industry or regulatory toolkits and control frameworks or standards.	K1 K2 K3 K4 K5 K6 K7 K8 K9 K11 K12 K14 K15 S1 S2 S3 S9 S12 B1 B2 B3 B5 B6

KSBs

Knowledge

K1: Relevant regulatory and legislative requirements such as data protection, GDPR, confidentiality, cyber security, for the handling and processing of data and its application.

K2: Technology and software used to provide appropriate representation of data and manipulate them into formats (tables, graphs and portfolios) for publication.

K3: The processing of data in technology and software and risks associated with it.

K4: Risk assessment methodologies and approaches to risk treatment or mitigation pertaining to processing data and the impact to the business, recommending appropriate risk treatment or mitigation.

K5: The roles of the key stakeholders in their organisation and how they interact with their own role.

K6: Privacy by design principles and practices such as records of processing and data protection impact assessments (DPIAs).

K7: Fundamental rights of information requests such as Freedom of Information (FOI), Individual Rights (IR), Environmental Information Regulation (EIR), Data Interoperability and Data Protection (DP).

K8: Industry or regulatory toolkits and control frameworks or standards.

K9: How their role fits into the organisation, its governance structures and escalation and the impact that it has.

K10: How their role adds value and the benefit of it to the business

K11: Communication techniques and approaches to interact with a range of key internal and external stakeholders in order to meet their requirements including using current and emerging technologies to support communication.

K12: Role of the Regulators

K13: The value of feedback from those they regulate, and the beneficiaries of regulation such as stakeholders in informing future activities.

K14: The support requirements and training needs of their stakeholders.

K15: The need for continuous improvement of systems and procedures to ensure that regulatory requirements are met.

K16: The importance of horizon scanning for future changes and developments in relation to data legislation and case law interpretation.

Skills

S1: Use IT systems to manage, share and store information in accordance with data protection requirements and organisation policies.

S2: Communicate complex subjects in simple terms through different media (such as face to face meetings, emails, reports and presentations) to enable key stakeholders to understand what is required.

S3: Prepare documentation and materials for review and ratification.

S4: Working at times under time pressure, prioritising their workloads in order to raise and resolve areas of concern such as individual rights, breach management, FOI requests and information sharing.

S5: Being able to accept and deal with changing priorities related to both their own work and to the organisation, showing the flexibility to maintain high standards in a changing environment.

S6: Undertake data collection, data analysis, data presentation and date storage such as data incidents.

S7: Interpret regulation and legislation, share best practice and advise stakeholders on its application.

S8: Identify organisation needs and how these are applied to enquiries.

S9: Interpret and apply sector guidance appropriately.

S10: Undertake investigations and interviews in order to assess a data breach.

S11: Gather, analyse, use and share data to inform risk assessment and make judgements on actions to take.

S12: Make decisions on data protection and information governance issues raised and ensure that any areas of concern are escalated to the stakeholders.

S13: Provide day to day support, specialist advice, guidance and training across the organisation and external stakeholders for all matters regarding information governance and data protection.

S14: Identify potential data solutions and evidence the way in which they could improve data management.

Behaviours

B1: Acts in a professional manner with integrity and confidentiality.

B2: Works collaboratively with others across the organisation and external stakeholders.

B3: Has accountability and ownership of their tasks and workload.

B4: Seeks learning opportunities and continuous professional development.

B5: Works flexibly and adapts to circumstances.

B6: Takes responsibility, shows initiative and is organised.

Qualifications

English and Maths

Apprentices without level 2 English and maths will need to achieve this level prior to taking the End-Point Assessment. For those with an education, health and care plan or a legacy statement, the apprenticeship's English and maths minimum requirement is Entry Level 3. A British Sign Language (BSL) qualification is an alternative to the English qualification for those whose primary language is BSL.

Professional recognition

This standard aligns with the following professional recognition:

- Information and Records Management Society for Individual member grade
- The British Computer Society for Associate member grade

Additional details

Occupational Level:

4

Duration (months):

18

Review

this apprenticeship will be reviewed in accordance with our change request policy.

Version log

VERSION	CHANGE DETAIL	EARLIEST START DATE	LATEST START DATE	LATEST END DATE
1.1	Occupational standard and end-point assessment plan revised Amendment to S14 required to mitigate EPA delivery issues. Two grading descriptor have been amended to mitigate delivery issues.	19/08/2024	Not set	Not set
1.0	Approved for delivery	30/03/2022	18/08/2024	Not set