

Information Governance

Service Specification 2022

Information Governance Unit



Information Governance

Keeping your essential information safe and secure

The Information Governance Unit (IGU) offer advice, guidance and training on information and cyber security and compliance with the data protection law, including the Data Protection Act, UK General Data Protection Regulation and Subject Access Requests.

The Information Governance Service Level Agreement package can be tailored to your setting, and a tiered approach to service delivery, providing ultimate flexibility to suit specific needs.

Two tiers of service level are available with the lower tier being more an insurance service (just in case of issues) and the higher tier being a fully comprehensive questions and training package ideal for those wishing to ensure full compliance with the legislation.

The UK GDPR introduces a duty to appoint a Data Protection Officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities.

- Data protection is about ensuring people can trust you to use their data fairly and responsibly.
- If you collect information about individuals for any reason other than your own personal, family or household purposes, you need to comply.
- The UK data protection regime is set out in the DPA 2018, along with the GDPR (which also forms part of UK law). It takes a flexible, risk-based approach which puts the onus on you to think about and justify how and why you use data.
- Failure to comply can result in a monetary penalty from the Information Commissioners Office.

The Data Protection Officer does not just advise on the law.

They must have many skills including liaising with senior management, driving change, influencing organisational culture, devising compliance strategies, delivering training, designing, and conducting audits, advising on DPIAs and liaising with the Information Commissioner.

Advice Line

The IGU team are on hand for advice via telephone and email 5 days a week, plus an out of hours number for emergencies.

Standard SLA – Tier 1 £265 + VAT per annum

Data Protection, Information and Cyber Security

This first tier in the Information Governance SLA offer ensures that care homes with policies, procedures and processes already in place, have access to day-to-day advice on the following topics:

CCTV	Information Security Policy
Consent	Information Security Report
Data Breach*	International Transfers of data
Data Flow/Mapping	Privacy Notice
Data Protection Impact Assessment (DPIA)*	Redaction
Data Protection Policy	Retention
Freedom of Information	Subject Access Request (SAR)*
Information and Cyber Security	Third Party Contractors
Information Asset Register	

*These topics receive further specialist support under Tier 2 DPO SLA

It is expected that any care home purchasing this package will already have an independent Data Protection Officer (DPO) appointed.

Please note: The DPO must be an expert in data protection, adequately resourced and report to the highest management level. They can be externally appointed or an existing employee. If your DPO is a care home employee, they must be impartial. Anyone whose role involves handling or processing any information held by the care home would have a conflict of interest and would not be suitable to act as DPO.

E-Bulletins

All care homes purchasing this package will receive a monthly e-bulletin containing relevant advice, updates on guidance or legislation and any data protection news specifically related to the Care Home Sector.

Training

Annual on-line training in Data Protection, Information Security and Cyber Security with a recording made available if unable to attend

Specialist SLA – Tier 2 (DPO Service) £400 + VAT

Data Protection, Information and Cyber Security and Provision of a DPO

The UK GDPR introduces a duty to appoint a Data Protection Officer (DPO) if you are a public authority or body, or if you carry out certain types of processing activities. If you are unsure whether your organisation requires a DPO please complete the screening questions at this link:

[Do I need a Data Protection Officer \(DPO\)? | ICO](#)

A DPO must be independent, an expert in data protection and adequately resourced.

A current member of staff could be appointed (however there should not be a conflict of interest) or can be an external to your organisation.

Several organisations can have a shared DPO.

This second tier of the Information Governance SLA offer is designed to complement the tier 1 with the provision of a named Data Protection Officer and specialist support in areas where statutory timeframes, or specific legal obligations exist.

Includes everything in Tier 1 as well as the following specialist support and the tasks of a Data Protection Officer

- Informing/advising on obligations to comply with GDPR via email updates
- Provide a named Data Protection Officer (DPO)
- Specific guidance and advice provided by specialist GDPR Practitioners on how to handle, respond, record and report in the following areas:

Data Protection Impact Assessment (DPIA)
Data Breach
Subject Access Request (SAR)

Data Protection Officer

The DPO is an independent monitoring and advisory role that supports your Care Home towards compliance with the law.

Named Contact

In providing a named DPO for publication in Care Home policies, this enhanced package provides a professional point of contact for liaison with the Information Commissioner's Office (ICO).

Information Security Health Check

Available on request, this health check comprises of a half day on-site visit and the production of an Information Security report and action plan (virtual for Out of County). A member of the team will step through reviewing security aspects of the care home, the report will provide an outline with recommendations for appropriate action and measures to mitigate any risks found.

Advice Line

The IGU team are on hand to provide support and advice via telephone and a dedicated DPO email inbox 5 days a week, plus an out of hours number for emergencies.

NOTE – this service is advisory, ultimately decisions are the responsibility of the data controller, i.e., the Care Home

GDPR GAP Analysis –£160

GDPR Gap Analysis comprises of a one-off on-site or virtual assessment of a care home's existing data protection practices (virtual for Out of County). This service can also be purchased on its own.

Gap Report

The Gap Report highlights areas of strength and tackles areas for development with a prioritised plan of action. Advice, supporting information and document templates will be provided to assist the care home towards compliance.

Training for DPO's who are employed by a care home –£75 + VAT per delegate

IG Team to offer an on-line training session to include:

- What Care Homes need to have in place to be compliant with data protection legislation
- The role of DPO and all tasks they are responsible for
- Principles of data protection as defined by UK-GDPR and legal basis
- Privacy Notices
- Data Protection Impact Assessments, what to look out for and managing risks, due diligence, and accountability
- Advice on training, raising awareness and completing audits
- ICO and their powers
- Investigating Information Security Incidents and when to report to Information Commissioner's Office, includes steps
- Overseas transfers
- Reducing risks
- Developing a systematic/programme approach to compliance
- Developing a communication strategy
- Handling conflicts of interest
- Where to find resources to assist in the DPO role

Learning Objectives:

Understand the importance of their role

Discuss and identify the practical key skills required to be a successful DPO

Understand the context of delivering a Data Protection Programme

Discuss the challenges in their role and the solutions

On-Site Data Protection Training or Information Security for all staff £100 per hour (plus expenses) Unlimited attendees.

Bespoke training/workshops are also available - Quote applies

***The care home remains the Data Controller as identified by GDPR and is the main decision maker regarding processing of personal data.**

***Recommendations will be made to ensure compliance; however, the care home is ultimately liable for any decisions or fines which may arise from the Information Commissioners Office.**

*** Payment will be invoiced annually on sign up**

Overview of Tiers

Subject	Tier One	Tier Two
	Standard SLA	DPO Service
	General day to day advice	Specialist support
CCTV	✓	✓
Consent	✓	✓
Data Breach	✓	✓
Data Flow/Mapping	✓	✓
Advice on Data Protection Impact Assessment	✓	✓
Data Protection Officer (DPO)		✓
Data Protection Policy	✓	✓
E-Bulletin	✓	✓
ICO Liaison		✓
Information and Cyber Security	✓	✓
information Security Health Check		✓
Informing/advising on obligations to comply with GDPR via email updates		✓
Information Asset Register	✓	✓
Information Security Policy	✓	✓
Information Security Report	✓	✓
International Transfers of data	✓	✓
Privacy Notice	✓	✓
Redaction	✓	✓
Retention	✓	✓
Sign off on data protection impact assessments		✓
Sign off records of processing		✓
Subject Access Request (SAR)	✓	✓
Third Party Contractors	✓	✓
Assist with monitoring compliance of Data Protection Legislation, policies, training completion, raising awareness and audits		✓