IT Governance

Small GDPR Gap Analysis

Service description-Europe

Protect • Comply • Thrive

Understand your GDPR compliance position

The GDPR gap analysis service assesses your organisation's current level of compliance with the Regulation, and helps identify and prioritise the key work areas that your organisation must address to be compliant.

Consultancy fee

The price for the GDPR gap analysis service is €2,320 (or local currency equivalent), excluding VAT.

The fee excludes any necessary travel, accommodation and subsistence expenses. Expenses will be assessed and charged in arrears.

Service eligibility

The service package is applicable to small organisations with up to 20 staff and with all the key personnel (senior management, HR managers, compliance, IT, sales, marketing, and procurement) based at a single site. The service can be delivered to organisations in any sector or industry.

For organisations that fall outside the eligibility criteria, please contact us on +00 800 48 484 484 for a quotation.

Resource requirements

- You will need to provide essential information for the project to proceed on schedule and fulfil its objectives. This will be managed to minimise any disruption, but it is essential that your staff give any requests the appropriate priority.
- You will need an internal project coordinator to host the meetings and to ensure all required information is provided on time, and that tasks and actions allocated to your staff are carried out as agreed.

Service description

You will be assigned a GDPR consultant who will assess your organisation's privacy management and data protection practices through an on-site review of the following areas:

1. **Data protection governance** – the extent to which data protection accountability, responsibility, policies and procedures, performance measurement controls, and reporting mechanisms to monitor compliance are in place and operating throughout the organisation.

2. **Risk management** – the corporate arrangements in place for privacy risk management across the organisation, the extent to which the corporate risk regime incorporates information-specific risks, and which risks to the rights and freedoms of natural subjects are addressed.

3. GDPR project – the extent to which an appropriately staffed, funded and supported GDPR project is in place, and capable of delivering realistic objectives to ensure compliance by 25 May 2018.

4. Data protection officer – whether a DPO is mandatory, a DPO been appointed, the role is positioned appropriately and the DPO is capable of delivering against the GDPR requirements.

5. Roles and responsibilities – the extent to which roles and responsibilities are defined and established through the organisation, including necessary training and awareness.

6. Scope of compliance – it is essential that the scope of compliance is clearly defined, and takes account of all data processing in which the organisation has a role, whether as a data controller or as a data processor, as well as any data sharing activity. In order to determine the scope of compliance, we also have to identify all the important databases that hold personal data, as well all extra-territorial/trans-border processing.

7. Process analysis – for each process that involves personal data, it is essential to identify the extent to which each of the data processing principles is established. The lawful basis for processing is a key area of consideration. Are there any processes for which a data protection impact assessment (DPIA) is mandatory, and for which processes might a DPIA help establish data protection by design and data protection by default?

8. Personal information management system (PIMS) – demonstrating GDPR compliance requires a wide range of documentation. The scale of the documentation should be appropriate to the size and complexity of the organisation. The PIMS should also address staff training and awareness.

9. Information security management system (ISMS) – the technical and organisational measures that ensure adequate security of personal data, whether it is held in hard copy or electronic form, or processed by the organisation's systems. This includes a review of methodologies for testing security, and established cyber security certifications, standards and codes of practice.

10. Rights of data subjects – the organisation needs processes that will enable it to both facilitate and respond to data subjects exercising any or all their rights.

The on-site review will last one day.

GDPR compliance report

The report will identify in detail the extent to which your organisation meets the GDPR requirements in each of these areas, and will provide an action plan that identifies and prioritises the key issues that your organisation must address to be compliant. The report will be delivered within ten days of completing the data-gathering phase of the project.

Why choose us?

- We have an in-depth understanding of the GDPR requirements and how they should be met.
- We provide a complete compliance support service to help organisations prepare for and adapt to the GDPR:
    - Data flow audit
    - Gap analysis
    - Data protection impact assessments (DPIAs)
    - Bespoke transition services
- Our specialist team has extensive data protection and information security management project expertise, both in the UK and overseas.
- Our transparent proposals are fixed price, so you won't get any unexpected surprises.
- You will have access to a dedicated account manager throughout the project.

Speak to an expert

Call our data protection team on **00 800 48 484 484** for further information and to discuss your GDPR project requirements.