Aristi

Cyber Security
Made Simple.

End to end cyber security services to protect your **data, technology and reputation.**

# ARISTI
# GDPR SERVICES

30 JANUARY 2026

Aristi Limited, Innovation Centre, 1 Devon Way, Longbridge Technology Park, Birmingham B31 2TS
Web: www.aristi.co.uk Email: info@aristi.co.uk Tel: 0121 222 5630

# 1 CONTENTS.


1 Contents. 1
2 Executive Summary. 2
3 Our GDPR Service Offering 3
3.1 Overview 3
3.2 GDPR Readiness Assessment 3
3.2.1 Assess 3
3.2.2 Engage 4
3.2.3 Plan 4
3.2.4 Delivery 4
3.3 GDPR Implementation 4
3.3.1 Progress the Plan 4
3.3.2 Review 5
3.3.3 Delivery Plan 5
4 Data Protection Impact Assessment (DPIA) 6
4.1 Overview 6
4.2 SCOPE OF THE DPIA 6
4.3 METHODOLOGY AND APPROACH 6
4.4 Delivery Plan 7
5 Virtual Data Protection Officer (vDPO) Service 8
5.1 vDPO Service Overview 8
5.2 vDPO Service Definition 8
5.3 Prerequisites 9
5.4 On Boarding 9

# 2 EXECUTIVE SUMMARY.

Aristi is a cyber security and data protection services provider to the public and private sectors. Our cyber security services are approved by the National Cyber Security Centre (NCSC)[1], the government department responsible for keeping the UK's critical services safe from cyber-attacks. We provide a comprehensive range of professional services include GDPR training and implementation, security awareness training for senior management and staff, development of data management and governance structures, development of information risk management processes, technical vulnerability assessments/penetration tests, cyber risk exposure assessments, cyber resilience assessments, social engineering tests and security audits.

Since 2008, when Aristi was established, we have been helping our clients to comply with the UK Data Protection Act and build good practices for data management. We deliver GDPR training courses from our offices, remotely over MS Teams and on site, for senior management, data controllers, data processors and users involved in the management of personal information.

Our consultants have worked with some of the most sensitive data in the UK through our engagements with industry, Critical National Infrastructure (CNI), government and emergency services. We have provided support to service providers to help build secure cloud environments for holding sensitive personal data for UK police forces, HMG to develop risk management processes for UK emergency services including the management of personal data. We have we have helped our clients to implement GDPR compliant data management processes and provide ongoing managed services to help maintain compliance. This knowledge and expertise allows us to support our clients more effectively and provide pragmatic security advice and guidance.

We believe that good data security is that which is embedded into the organisation and is proportionate to business requirements, becoming a business enabler rather than a barrier to innovation. Security is not just about implementing technical controls. Effective security is about instilling good practices within the organisation, changing the behaviour of staff and implementing a governance structure that delivers an excellent user experience where security is 'good enough' to protect important information assets.

Our approach to GDPR is based on our experience of information security and helping ensure that good practice becomes part of 'business as usual'. This requires senior management to recognise that personal information and ownership of the associated risks is their responsibility and not that of IT. The business owns the data, so the business needs to take accountability for data and manage those who access it. GDPR is about applying good practice and changing the behaviour of staff so that they instinctively do the right thing.

Our aim is to become a trusted partner to our clients, so you can call on our support whenever you need it. Our consultants will work closely with you to share their knowledge and experience at every stage of the engagement.

[1] https://www.ncsc.gov.uk/information/about-ncsc

# 3 Our GDPR Service Offering

## 3.1 Overview

Our GDPR service offering is shown in figure 1 below and is designed to provide a complete package of support to help our clients meet the requirements of the legislation.

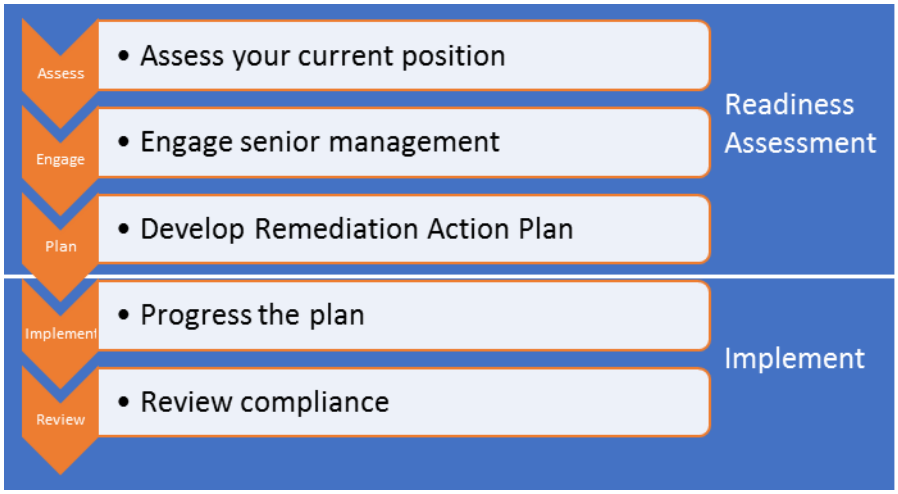


**Figure 1. Aristi GDPR Service Offering**

## 3.2 GDPR Readiness Assessment

### 3.2.1 Assess

The first phase involves conducting a GDPR Gap Analysis to assess the current level of compliance. This consists of an assessment of existing processes and policies relating to the management of personal data against the requirements of GDPR. This is conducted on site at the client's offices.

The assessment also includes interviews with department heads/information asset owners typically lasting 30 to 40 minutes each. The aim of the interviews is to establish current working practices and personal data management requirements.

The assessment tasks include the following:

- Review existing Data Protection processes, practices and systems to highlight areas and gaps that need to be addressed for compliance with current legislation and the GDPR;
- Produce an overview of what is currently in place relative to GDPR requirements;
- Set out risks with current data processing practices;
- Identify high risk processing activities;
- Identify any 3rd party contracts, Service Level Agreements (SLAs) impacts and how impacts can be addressed;
- Assess if the technical infrastructure is appropriate and proportionate to meet the requirements of the GDPR;

- Prioritise any gaps identified as part of the assessment of the technical infrastructure.

#### 3.2.2 Engage

The second phase is to document the findings in a formal report together with recommendations. The report is presented on site to senior management and other relevant stakeholders to make them aware of the current state of compliance, the implications and what needs to be done next. This also provides the opportunity for stakeholders to ask questions and gain clarification on the findings and recommendations.

#### 3.2.3 Plan

The final phase involves the development of a Remediation Action Plan (RAP) to address the recommendations detailed in the report. The RAP details the tasks that need to be completed and the time required for each task. This effectively forms the roadmap for compliance ensuring the timescales for compliance are met.

#### 3.2.4 Delivery

The GDPR Readiness typically takes around 5 days, but this is dependant on the size and complexity of the organisation. We can deliver the engagement on site or remotely over MS Teams.

### 3.3 GDPR Implementation

#### 3.3.1 Progress the Plan

A meeting is held with the client to assign resources and timescales to the RAP. We then work with the client to progress the RAP. This includes the development and implementation of all required Data Protection Policy documentation and processes. In order to save costs for the client, we aim to use any existing relevant documentation already in place supplemented by templates from our GDPR toolkit, ensuring at all times that they are fit for purpose.

The implementation at a minimum, includes the following:

1. Development of GDPR compliant process/plans for
    a. Data breach incident response and responsibilities of staff when/if dealing with same
    b. Subject access requests
    c. Requests for rectification
    d. Requests for erasure
    e. Data transfers
    f. General data protection policies e.g. retention policy
2. Development of a methodology for conducting Data Protection Impact Assessments (DPIAs).
3. Documented review and prioritisation of technological infrastructures to support ongoing GDPR compliance
4. Development of a template Register that would include the types of personal data held and an appropriate retention schedule (bearing in mind some retention periods are set out in legislation)

In order for compliance to be sustainable, staff involved in the management of personal data will need to be made aware of the new processes and how to follow them. This can be communicated through training workshops allowing staff to ask questions and fully engage in the subject matter. We can also develop a communications plan to use channels such as Intranet, Emails or newsletters to inform staff of the new processes and why they need to be followed.

We can also run our one-day GDPR Awareness course on site for senior management and data owners to transfer key knowledge on the regulation and how to maintain compliance.

### 3.3.2 Review

Following implementation, a compliance review is conducted to ensure the requirements of GDPR are being met. This takes the form of an on-site audit to assess compliance with the new policies and procedures.

In consultation with the client, we can produce a strategy to maintain ongoing compliance against the requirements of the GDPR. This strategy at a minimum includes:

1. Methodologies to carry out future GDPR compliance reviews including monitoring and reporting on compliance with policies.
2. Template Policy documents including GDPR compliant retention policy, privacy policies, privacy statements, relevant aspects of customer service in relation to data protection.

### 3.3.3 Delivery Plan

Delivery of the implementation activity is dependent on the output from the Readiness Assessment. Our clients typically purchase a ‘pot’ of consultancy days (10 to 15 days is the norm) from which support can be called off as required. The client is only invoiced for the days used regardless of the number of days ordered.

# 4 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

## 4.1 Overview

Organisations that engage in processing activities likely to result in high risk to individuals are required to conduct a DPIA. This assessment helps ensure that privacy and data protection risks are identified early and addressed effectively through appropriate technical and organisational measures.

The purpose of these engagements is to:

- Evaluate current and proposed personal data processing activities.
- Identify and assess privacy and data protection risks.
- Recommend mitigation measures to reduce identified risks.
- Support informed decision-making and regulatory compliance.

## 4.2 SCOPE OF THE DPIA

The DPIA will cover the following areas:

- Description of processing activities, purposes, and legal bases.
- Categories of personal data and data subjects involved.
- Data flows, systems, vendors, and third-party processors.
- Assessment of necessity and proportionality of processing.
- Identification and evaluation of risks to data subjects.
- Review of existing controls and safeguards.
- Recommendations for additional risk mitigation measures.

Out-of-scope items, if any, will be explicitly documented and agreed upon prior to commencement.

## 4.3 METHODOLOGY AND APPROACH

Our DPIA methodology follows regulatory guidance and industry best practices, including guidance from the Information Commissioner's Office.

**Phase 1: Initiation and Planning**

- Kick-off meeting with key stakeholders.
- Confirmation of scope, objectives, and timelines.
- Identification of relevant documentation and systems.

**Phase 2: Information Gathering**

- Information gathering meetings with business, IT, security, and data owners.
- Review of policies, procedures, contracts, and solution documentation.
- Mapping of personal data flows and processing activities.

**Phase 3: Risk Assessment**

- Assessment of necessity and proportionality.
- Identification of privacy and data protection risks.
- Evaluation of likelihood and severity of impact on individuals.
- Consideration of risks related to confidentiality, integrity, availability, and data subject rights.

**Phase 4: Mitigation and Recommendations**

- Review of proposed technical and organisational measures.
- Development of recommended mitigation actions.
- Residual risk assessment following proposed controls.

**Phase 5: Reporting and Validation**

- Preparation of a formal DPIA.
- Presentation of findings to stakeholders.
- Incorporation of feedback and finalisation of the DPIA.

**5. Deliverables**

The engagement will result in the following deliverables:

- A comprehensive DPIA compliant with regulatory requirements.
- Data flow diagrams and processing descriptions (as applicable).
- Risk register detailing identified risks and mitigation measures.
- Executive summary highlighting key findings and decisions required.

## 4.4 Delivery Plan

Delivery of a DPIA typically takes 5 days but this can vary depending on the complexity of the scope of work.

# 5 Virtual Data Protection Officer (vDPO) Service

## 5.1 vDPO Service Overview

To support your on going GDPR compliance and management requirements, we can provide a Virtual DPO service.

You will have access to our vDPO team who have professional experience and knowledge of data protection and will act as the DPO for your business during the term of the engagement. The key responsibilities of the DPO are listed below:

- To inform and advise the client of their obligations to comply with the GDPR and other data protection laws;
- To monitor compliance with the GDPR, support the management of internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits;
- To be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc)[2].

The vDPO service provides a 'critical friend' to your business to provide support and guidance on GDPR and wider data protection including cyber security.

Under the GDPR, DPOs are not personally responsible for non-compliance. GDPR compliance is the responsibility of the business and assignment of a DPO must not be seen by the board as a means to be absolved from their responsibilities for data ownership and protection. The DPO is responsible for advising the board (and the data owners) on GDPR and how to comply with the regulation.

## 5.2 vDPO Service Definition

The Virtual DPO service includes the following:

- A DPO available to the client to provide advice and guidance on GDPR related issues;
- Option of monthly or quarterly GDPR audits conducted with client stakeholders to monitor compliance with GDPR and provide assurance to your board that your GDPR processes are effective;
- Telephone and email support Monday to Friday, 0830 to 1700 (excluding public holidays).

[2] This will be via an agreed client point of contact to enable such communications to be managed.

## 5.3 Prerequisites[3]

The Virtual DPO service is offered on the basis that the client has established the following:

- Compliance with the GDPR through development of the required processes, procedures and documentation;
- A governance structure to manage personal data through assignment of Data Owners and a risk reporting route to the board;
- A member of staff (can be more than one) who is responsible for the day to day management of personal information including:
    - Overall responsibility for the management of GDPR;
    - Approval of procedures for the management of personal information;
    - Management of requests from data subjects;
    - Management of data breaches.

## 5.4 On Boarding

This is a key phase of the engagement as it ensures that the DPO role is fully aligned to the business needs. As part of our onboarding process, we arrange a Project Initiation Meeting with the client to:

- Introduce the Aristi DPO and meet client stakeholders;
- Understand the business, its organisational structure, processes and working practices;
- Confirm common understanding of aims and objectives for the DPO;
- Confirm client representatives/ Points of Contact for the DPO;
- Confirm DPO lines of communication;
- Agree audit schedule

We achieve the above in a half day workshop held on site or remotely over MS Teams.

[3] Aristi can provide support to meet these requirements.