Cyber - Scope

Managed, Secured Networks Services

GDPR's Gap-Analysis

Delivering a targeted assessment of your compliance with the GDPR, our privacy experts provide a detailed assessment of your readiness, key gaps and risks and remediation roadmap

The GDPR gap analysis service provides an assessment of your organization's current level of compliance with the Regulation, to identify and priorities the key work areas that your organization must address

GDPR at a Glance:

The EU General Data Protection Regulation (GDPR) becomes a valid law across all EU members' states on 25th May 2018. The purpose of the new regulation is two folds:

1. To improve consumer confidence in organizations that hold and process their personal data by reinforcing their privacy and security rights consistently across the EU, and
2. To simplify the free flow of personal data in the EU through a coherent and consistent data protection framework across the member states.

Every organization that processes or shares personal data must comply with the new regulation. This involves organizations understanding what personal data they currently hold or process and the risks to that data, implementing tools and compliance, adapting their business processes and changing the way they collaborate with suppliers. Organizations found to be in breach of the regulation face administrative fines of up to 4% of their annual global turnover or 20€ million – whichever is the greater.

CyberScope is a qualified GDPR's practitioner (GASQ's certificate #983720), which provides wide portfolio of GDPR's professional services including Data-Flow Audit, Gap-Analysis, DPIA and DPO as a service.

Why Chose CyberScope

- ✓ GDPR Know-how we have an in-depth understanding of the GDPR and how it should be met in practice
- ✓ Experience Over 20 years of extensive IT/ Data-Security aspects while analyzing data networks infrastructures
- ✓ Qualification Our Practitioner are certified by GASQ
- ✓ Price best Value-for-Money
- ✓ Added-Value Valuable expertise in IT / Networks and Cyber-Security advanced solutions to mitigate data-protection risks

The GDPR covers the following areas:

- **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.
- **Risk management** – is privacy risk included in the corporate risk register? What corporate arrangements are in place for privacy risk management across the organization, to what extent does the corporate risk regime incorporate information-specific risks, and which risks to the rights and freedoms of natural subjects are addressed?
- **GDPR project** – the extent to which an appropriately staffed, funded and supported GDPR project is in place, and capable of delivering realistic objectives.
- **Data Protection Officer** – is a DPO mandatory, has a DPO been appointed, and is the role positioned appropriately and is the individual capable of delivering against the GDPR requirements?
- **Roles and responsibilities** – the extent to which roles and responsibilities are defined and established through the organization, including necessary training and awareness.
- **Scope of compliance** – it is essential that the scope of compliance is clearly defined, taking account of all the data processing in which the organization 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 databases that hold personal data as well as all extra-territorial/trans-border processing.
- **Process analysis** – it is essential to identify, for each process that involves personal data, the extent to which each of the data processing principles are established. 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?
- **Personal information management system (PIMS)** – there is a wide range of documentation that is required to ensure that the organization is able to demonstrate compliance with the requirements of GDPR. The scale of the documentation should be appropriate to the size and complexity of the organization.
- **Information security management system (ISMS)** – the technical and organizational measures in place to ensure that there is adequate security of personal data held in hard copy or electronic format or processed through the organization's systems. This includes a review of methodologies for testing security, and established cyber security certifications, standards and codes of practice.
- **Rights of data subjects** – the organization needs processes that will enable it to both facilitate and respond to data subjects exercising any or all of their rights.

Personal Data means "any information relating to an identified or identifiable natural person ('data-subject')". The regulation states this is also includes online identifiers such as IP address and cookies.

CyberScope will cover the below subjects through the Gap-Analysis process and will provide you with a clear report including actionable recommendations list on key areas to be corrected.
Below is a typical Gap-Analysis project:

Interfaces
A qualified GDPR's Practitioner will be appointed to interview the company's key personnel on-site and will liaise all activities with the company's GDPR's Project Manager. The GDPR's Project Manager will facilitate all the relevant information (Collected Personal-Data, Policies, Contracts with suppliers etc.) to be collected across the company.

Personal Data collection, law-full basis, means and purposes of data collection and processing by internal functions and external entities (i.e. suppliers) will be documented and analyzed. Frame-works and policies defining Access rights to personal data, networks infrastructure and applications used to collect, process, keep and erase will be analyzed and the company's ability to properly treat Data-Subject Access Rights (DSAR)

Thorough Analysis of the company's operation to identify a risk to rights and freedom of personal information will be conducted and how the company is prepared to manage a Data-Breach and in such case the policies required to identify the severity of such breach and in each case how to document internally or if required to inform Data-Subjects and Supervising authority

Compliance will be analyzed while monitoring the identified categories of Data collection and purpose of processing them as well as identify if a DPO (Data-Protection-Officer) shall be appointed and in case of a high-risk for rights and freedom of Data-Subject if a DPIA is required

The Report will identify in detail the extent to which the company meets GDPR requirements in each of these areas and will provide actionable-recommendation list that identify and prioritizes the key issues that the company must address.

Cyber - Scope
Managed, Secured Networks Services

CyberScope (the Cyber security & GDPR brand of Space-Band S.L.U)
NIF ESB 87829107
Retamar #3
San Sebastian de los Reyes
28708, Madrid
Spain
Tel +34 910 660 875