



**SERVICE METHODOLOGY
GDPR
GENERAL DATA PROTECTION
REGULATION**

INTRODUCTION TO GDPR

GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer data and personal data across EU nations. Some of the key privacy and data protection requirements of the GDPR include:

- Requiring the consent of subjects for data processing
- Anonymize collected data to protect privacy
- Providing data breach notifications
- Safely handling the transfer of data across borders
- Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

GDPR mandates regulatory requirements for all the companies that handle EU citizens' data to better safeguard the processing and movement of citizens' personal data.

KICKOFF

Kickoff meeting is an essential tool to communicate and plan for the execution of the project with minimal obstruction and to complete the project within planned time and cost.


Agenda for the kick off meeting is:

- Project plan discussion: This includes discussion about accountability and responsibility of stake holders, milestones and deliverables in the project.
- Scope of services
- Legal and regulatory requirements

CREATION OF CORE TEAM

- Appointment of Data protection officer (DPO)
- Appointment of Internal GDPR /GRC committee (Governance Risk & Compliance) (*If required)


GDPR AWARENESS TRAINING



GDPR awareness training will be conducted to the employees of your organization. The training session is to help employees to gain knowledge, understand the concepts of GDPR, and align processes and practice towards achieving and establishing, implementing, maintaining and continually improving a compliance based system work environment. When staffs have been trained they can think & act and contribute towards achieving the goals.

GDPR - PHASE WISE IMPLEMENTATION

PHASE I - GAP ANALYSIS



During this phase we conduct a gap analysis to check how much of your current practices are in line with the requirements. Your current practices are verified against the below two reference criteria,

- GDPR Requirements
- Legal, Regulatory and Statutory requirements

The results of this analysis are presented in the form of a Gap Analysis Report. This report acts as the list of action items for the remainder of the project.

PHASE II - INFORMATION FLOW ASSESSMENT

In this phase we help in identification of information sources, and the processing infrastructure that involves personnel, technology, and physical infrastructure with respect to GDPR.

PHASE III - DATA PRIVACY IMPACT ASSESSMENT (DPIA)

A Data Protection Impact Assessment (DPIA) is a process whereby potential privacy issues & risks are identified and examined from the perspective of all stakeholders. This allows the organization to anticipate, address the likely impacts of new initiatives through specific measures to minimize / reduce the risks. DPIA are designed to minimize the risk of harm that can be caused by the use / misuse of personal information by addressing data protection & privacy concerns at the design & development stage of a project.

We assist in developing a DPIA procedure and DPIA Register by coordinating with the functional head so that it should benefit the Organization by managing risks, avoiding damage to reputation, ensuring legal obligations are met and improving the relationship with stakeholders.

PHASE IV - SECURE PERSONAL DATA TRANSFER ANALYSIS

We help in Analyzing what personal data is being transferred outside of your company and when also we also assist in designing of necessary security measures to adequately protect personal data and also the personal data that is transferred outside of the company.

PHASE V - SETTING UP PROCESS FOR DATA BREACH INCIDENTS

We assist in Setting up the processes to identify and handle personal data breaches. (Eg.Data breach notification procedures) and also assist in developing procedures on incident reporting mechanism to the concerned supervisory authority.

PHASE VI - DOCUMENTATION SUPPORT


We assist in Implementation of necessary organizational and technical measures to protect the personal data of data subjects and also help in assisting on designing relevant documentation with controls policies and procedures that ensures that GDPR is well embedded in the organization processes.

DATA PROTECTION OFFICER INTERNAL AUDIT TRAINING

GDPR Internal Auditor (IA) Training will be provided to the DPO. This training will equip such personnel to analyze the need for IA, plan and schedule IA, prepare audit checklists, and conduct an IA and to document and report their observations to the top management




GDPR INTERNAL AUDIT



Our experts will oversee the conducting of internal audit by your DPO. This internal audit will identify still existing gaps in the system and demonstrate the level of preparedness to face the compliance audit. This audit gives the organization a chance to identify and rectify all non-conformances before proceeding to the compliance audit. The top management is notified of the internal audit findings.

GDPR - ROOT CAUSE ANALYSIS (RCA) AND CORRECTIVE ACTIONS




All non-conformances identified during the internal audit, client or third party audits, or from Risk Register, DPIA register, Incident logs, Data Backup logs, Data Breach notification reports, Vulnerability Assessment & Penetration Test (VAPT), Data retention logs and any other sources have to be listed.

RCA is performed using techniques like Brainstorming and Fish-Bone methods. The optimal correction and corrective actions are implemented and the effectiveness of such actions is documented and reviewed via a GDPR Corrective Action Report (CAR)

Our experts will be present with your team to guide through the process.

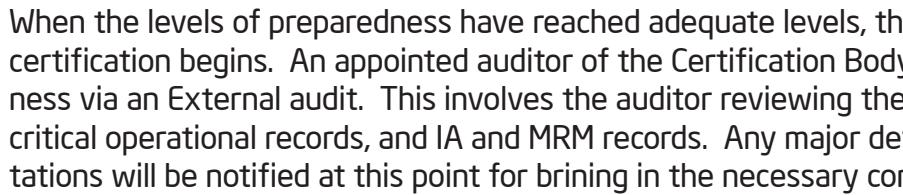
GDPR MANAGEMENT REVIEW MEETING (MRM)



The MRM is an opportunity for all stakeholders to meet on scheduled intervals to review, discuss and plan actions on the below agenda points,

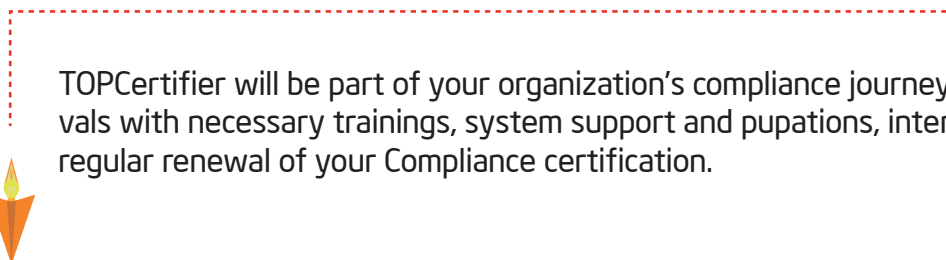
- DPIA reports
- Deviations on compliance aspects
- Post-delivery activities reports
- Action plan to resolve any open items
- Opportunities for improvement and changes needed in the system

GDPR COMPLIANCE AUDIT



When the levels of preparedness have reached adequate levels, the process for Compliance certification begins. An appointed auditor of the Certification Body (CB) verifies the preparedness via an External audit. This involves the auditor reviewing the policies, processes, SOP's, critical operational records, and IA and MRM records. Any major deviations from the CB's expectations will be notified at this point for bringing in the necessary corrections. This reduces the chances of major non-conformances during the certification audit. TOPCertifier will by liaise with all stakeholders and oversee smooth completion of the audit.

CONTINUATION OF COMPLIANCE



TOPCertifier will be part of your organization's compliance journey and assist you at regular intervals with necessary trainings, system support and pupations, internal and external audits and regular renewal of your Compliance certification.