Assessment of working practices

Convey GDPR key messages to stakeholders and the potential impact pertinent to the business. Familiarise and train staff to conduct privacy impact assessments for GDPR in scope data.

We will deliver:

Awareness training sessions, "train the trainer", education pertinent to your business.

01.

Roles & Resonsibilities

Designate either a Data Protection Officer, or Data Steward within the business to take responsibility for data privacy compliance. Agree future governance processes where the defined role can influence how data assets are used within the business

We will deliver:

Designation of role, job role definition, and author ongoing terms of reference governance.

02.

Data Asset Inventory

Conduct a data discovery exercise to determine what personal data is held and processed.

We will deliver:

Data map, basic data classification scheme with rules for each classification. Gap analysis between "as-is" and what compliance looks like. Advice as to how to ratify anecdotal data map using technology.

03.

Consent Mechanisms

Identify any exemptions that may be applicable for legacy data. Derive new policies for obtaining consent and explicit opt-out messages.

We will deliver:

Data Consent Matrix appended to classification map.

04.

Assessment of working practices

Document the legal basis for each data processing activity. Identify key risk areas and applicable compliance requirements for each business function.

We will deliver:

Risk Matrix showing (for each classification of data), identification of key risk areas and applicable compliance requirements. To include third parties.

05.

Security Controls

Assess whether personal data is processed securely and adequately protected. Work with the cyber security function and other business functions to ensure appropriate security controls are implemented commensurate with the risk and impact to individuals if lost.

We will deliver:

Technical risk register for each data processing activity together with recommended mitigations.

06.

Data Breach Reporting

Review people, process and technology to determine the capability to detect, report and investigate data breaches.

We will deliver:

Policy and governance amendments, incident response policy.

07.

Communication

Review current privacy notices, identify policy gaps and author new compliant policies whilst retaining business objectives.

We will deliver:

Policy gap analysis, remediate all privacy policies, notices, and opt-outs.

08.

Subject Rights

Review procedures to measure compliance with the rights of individuals (e.g. data portability, right to be forgotten).

We will deliver:

Gap analysis showing "as-is" ability of existing systems against compliance.

09.

Governance

Whilst maintaining business objective focus, define regular governance tasks and reporting to demonstrate continuous compliance.

We will deliver:

Creation of a data privacy governance structure bespoke to the business.

10.

ilicomm Technology Solutions

The GDPR Journey

10 steps to compliance

FOR MORE ON THE GDPR

www.ilicomm.com/**getting-ready-for-the-gdpr** +44 (0)121 289 3434

Information Security Management System
ISO 27001
Certified IS 640314

ilicomm
Technology Solutions