General Data Protection Regulation
What can you expect from the assessment process?

GDPR Readiness Checklist

This checklist will provide you with a detailed understanding of what we will be covering during the GDPR Readiness Assessment. If you don't have any of this in place already, don't panic; we will provide you with training, templates and guidance required.

Awareness:

○ We understand how personal data is defined within our country's data protection legislation.

○ We have identified whether we need to comply with the new General Data Protection Regulation.

Leadership:

○ We have identified who has overall responsibility for security and data protection within our organisation.

○ Management consider information security and data protection when reviewing performance.

Policies and Procedures:

○ We have procedures in place to mitigate risks.

○ We have procedures in place to monitor compliance.

○ We have created a personal data and information security training programme for employees.

○ We have a Privacy Notice.

○ We have identified who is responsible for ensuring compliance is maintained.

Roles and Responsibilities:

○ We have identified who is responsible for data security.

○ We have a Data Protection Officer (if required).

Data Mapping:

○ We have completed a data analysis.

○ We have completed a data flow audit.

○ We have put processes in place for all of the data that requires protection.

○ We have documented where the personal data we hold has been obtained from.

○ When assets are no longer required, we ensure data is securely wiped or destroyed.

Data Controllers:

○ We have put contracts in place for our data processors.

Data Processors:

○ We have put contracts in place for our sub-processors.

Risk Assessments:

○ We conduct risk assessments for data privacy.

○ We ensure data is encrypted before being stored or accessed by our public cloud provider.

○ We ensure our public cloud provider securely stores the data we share and hold.

○ Consent is obtained before personal data is stored outside of the European Economic Area (EEA).

Privacy Impact Assessment:

○ We carry out Data Protection Impact Assessment (DPIA) when required.

○ We consider data privacy when starting new projects to ensure that data is considered and protected, as part of the initial design.

Subject Rights:

○ Data Protection is referenced within our employee contracts.

○ Our policies and procedures clearly explain responsibilities for handling personal data.

○ We collect personal data in a fair, lawful and transparent manner.

○ We ensure data notices can be easily accessed by data subjects.

○ We obtain parental consent when subjects are under 16 years.

○ We are able to respond to Subject Access Requests (SAR's) within appropriate time-scales.

○ We ensure data is accurate and kept up-to-date.

○ We can delete data subject's personal data, when required.

○ We can stop processing personal information, when required.

○ We can provide electronic copies of an individual's personal data, when required.

○ We have a complaints and appeals procedure.

Legal Basis for Processing:

○ We document the legalities surrounding the reasons why we obtain personal information.

○ We record the ways in which we obtain consent for the purpose of demonstrating compliance.

Data Security:

○ Personal information is handled in a way that is appropriate to its sensitivity and confidentiality.

○ We ensure the level of data access granted to employees is appropriate to their position.

○ We complete security assessments.

○ We document security breaches involving personal data and report this, where appropriate.

Data Processing:

○ We ensure personal data is relevant and adequate for the organisation's purposes.

○ Our Data Privacy Statement includes a point of contact for issues concerning data protection.

○ Data subjects are able to revoke consent for data obtained.

○ We record the reasons why personal data was obtained.

○ Our contracts state whether we are acting as the data controller or data processor.

○ Our security policy is detailed within the relevant contracts.

○ Privacy impact assessments are carried out on new systems and projects where personal data is used.

Performance:

○ We record which processes/policies/technologies need to be monitored.

○ Senior level management review the output of monitoring activities.

Continual Improvement:

○ We identify nonconformities to help us continue improving our Privacy Management System.