**Project checklist for EU GDPR implementation**

|  |  |  |
| --- | --- | --- |
| **Implementation phases** | **Tasks** | **Done** |
| *Establish the project* | Decide whether you are going to use consultants, or if you will be using documentation templates. |  |
| Download the EU GDPR full text. |  |
| Conduct the GDPR Readiness Assessment to help you determine at which stage of the project implementation you are. |  |
| Educate your project team. |  |
| Write the Project Plan, including the definition of the project manager, project team, project sponsor, required resources, and milestones. |  |
| Define which stakeholders need to be informed about each step in the project. |  |
| Organise kick-off meeting. |  |
|  |  |
| *Develop top-level policies* | Establish the EU GDPR Personal Data Policy Framework. |  |
| Write the Personal Data Protection Policy. |  |
| Write the Employee Personal Data Protection Policy. |  |
| Write the Data Retention Policy. |  |
|  |  |
| *Organise your data protection* | Appoint a Data Protection Officer.  |  |
| Define the Data Protection Officer’s job description. |  |
|  |  |
| *Build up data inventory* | Write the Inventory of Processing Activities. |  |
| Maintain and update the Inventory of Processing Activities. |  |
|  |  |
| *Managing data subject rights* | Define the legal basis of the company to process personal data, and whether you need consent from the data subjects.  |  |
| Define data subject rights.  |  |
| Define and implement data subject consent forms. |  |
| Define and implement the Data Subject Access Request Procedure and develop a guide outlining how to deal with the requests. |  |
|  |  |
| *Data Protection Impact Assessment (DPIA)* | Define and write the Data Protection Impact Assessment Methodology (DPIA). |  |
| Maintain the DPIA Register.  |  |
| Set up a DPIA review schedule. |  |
|  |  |
| *Personal data transfers* | Develop the Cross-Border Personal Data Transfer Procedure. |  |
| Identify all of your suppliers based outside the European Economic Area (EEA) that will have access to personal data. |  |
| Prepare and sign Data Transfer Agreements for all identified suppliers outside of the EEA. |  |
|  |  |
| *Third-party compliance* | Identify the suppliers that process personal data on your behalf (data processors). |  |
| Prepare and sign agreements with data processors to ensure they will act based on your instructions and will comply with EU GDPR. |  |
|  |  |
| *Personal data protection* | Identify and implement adequate security measures to protect personal data. |  |
| Test and review the implemented measures on a regular basis. |  |
|  |  |
| *Handle data breaches* | Identify the key stakeholders and establish your “Data Breach Response Team.” |  |
| Establish a process to evaluate a data breach, and to notify the Supervisory Authority and data subjects. |  |
| Establish a process to respond to a data breach. |  |
| Maintain a record of all data breaches. |  |
|  |  |
| *Awareness presentations and trainings* | Define which competencies your employees need. |  |
| List the trainings your employees should attend. |  |
| Develop a training plan for the next few months. |  |
| Perform periodic security awareness trainings for all of your employees. |  |
|  |  |

For all the documents needed to comply with EU GDPR, check out this [EU GDPR Documentation Toolkit](https://advisera.com/eugdpracademy/eu-gdpr-documentation-toolkit/?utm_source=project-checklist-for-eu-gdpr-implementation&utm_medium=downloaded-content&utm_content=lang-en&utm_campaign=paid-toolkit-eugdpr).