GDPR audit checklist

Take the uncertainty out of your next GDPR audit by following these steps.

- [ ] **1. Understand the GDPR requirements**
Familiarise yourself with the key aspects of the GDPR, including the relevant data protection principles, rights of data subjects, data processing requirements, and security measures.

- [ ] **2. Form an audit team**
Assemble a team with cross-functional expertise on the privacy areas you are assessing, for example this may include your data protection officer and someone from legal, data governance, AI, IT, HR, marketing, etc.

- [ ] **3. Conduct data mapping**
Identify and document all data processing activities, including data collection, storage, and sharing across departments and systems. Understand which entities are responsible for data processing, both within your organisation and with third-party processors or other controllers.

- [ ] **4. Assess legal basis for data processing**
Evaluate and ensure that the correct legal basis has been chosen for the processing of the personal data and make sure you comply with the specific requirements for using that legal basis.

- [ ] **5. Evaluate data subject rights compliance**
Check that procedures are in place to handle data subject rights requests. Ensure that your GDPR audit checks the application of the data subject rights and how your organisation handles these. Also review policies, procedures and processes in place for handling data subject rights.

- [ ] **6. Review data processing agreements and GDPR clauses**
Ensure that all contracts with third-party vendors who process personal data on your organisations' behalf as a "processor" include GDPR-compliant clauses and full details of the personal data being processed. For any cross-border data transfers, ensure that appropriate safeguards, for example, Standard Contractual Clauses or Binding Corporate Rules are in place.

- [ ] **7. Examine data breach management processes and procedures**
Ensure that processes are in place for detecting and handling personal data breaches within the mandatory 72 hour time period. Review your organisation's policies, procedures and templates and ensure these are tested regularly.

- [ ] **8. Review data retention policies**
Ensure that personal data is retained for no longer than necessary and that there are clear data retention and deletion policies in place. Review if these are followed and personal data is being deleted or anonymised when no longer needed.

- [ ] **9. Data protection by design and default**
Ensure privacy is embedded into business processes. Review templates for data protection impact assessments (DPIAs). Look at if DPIAs are being carried out, reviewed and maintained to ensure they stay up to date.

- [ ] **10. Train employees and raise awareness**
Review any existing training requirements in relation to data protection and the GDPR. Check that the training is offered on induction and regularly thereafter.

- [ ] **11. Document findings**
Keep detailed records of your audit findings, actions taken, and areas for improvement.

- [ ] **12. Prepare a remediation plan**
Based on the audit findings, implement corrective actions to address any gaps or non-compliance issues. Assign owners for any privacy actions and make sure these are followed up to ensure that the privacy risks are mitigated.

HelloDPO

Your **data protection** team