

Compliance with Data Privacy legislation (from an SAP perspective)

Ten recommendations for your journey

Based on our experience in implementing compliance solutions for SAP[®] customers, we recommend the following:



1. Undertake a Data Privacy Impact Assessment (DPIA).

- Get your auditors and legal council involved early; they provide guidance on key risk areas and will provide a recommended framework for ongoing compliance management.
- Establish a privacy programme management team. At a minimum appoint a Data Protection Officer and register them with the Information Regulator.
- Assessments would be likely to include:
 - Personal information inventory and data flow mapping (per business area)
 - Privacy gap assessment
 - Third-party due diligence reviews



2. Increase awareness of relevant Data Privacy legislation.

- Undertake a privacy culture assessment to identify employee readiness and understanding and ensure customer-facing employees are well versed in associated rights
- Educate your employees and stakeholders on relevant data privacy legislation, what is required, and their associated responsibilities (leverage commercially available eLearning solutions, to accelerate adoption).
- Join professional privacy bodies – to leverage best practice approaches such as the International Association for Privacy Professionals (IAPP.org)



3. Undertake an audit of where sensitive data is stored within your SAP systems.

- Analyse your SAP environment to determine key areas where all the personal and sensitive data is stored. Processing requests and disclosing personal information will be difficult without a clear idea as to where sensitive data is stored.
- SAP functional teams should be aware of where sensitive data is stored in your SAP systems (including integrated components like Workflow, SAP BW, Change Documents etc) so that procedures for displaying and potentially removing the data can be developed/designed.
- Review your business process flows/blueprints and identify steps where sensitive data (customer, employee, supplier, business partner information) is available.



4. Reduce sensitive data on your non-production SAP systems.

- Reduce your risk profile by intelligently masking data in non-production systems. By taking your test systems out of the equation, you can reduce risk and overhead when handling requests.
- Look for unused clients/systems with sensitive data which can be deleted; or sensitive data which is not required in certain test clients and could be removed.



5. Secure your infrastructure.

- Check the SAP One Launchpad regularly for security patches specific to your SAP versions, Operating System and Database type.
- Ensure there is clear accountability within your SAP team for reviewing and applying SAP notes.
- Ensure your team has relevant skills to protect systems and hybrid cloud estates including Cloud and firewall rules.



6. Review or implement data retention policies to reduce historical data (within SAP).

- Develop an archiving/redacting and data retention policy framework for managing historical data which clearly indicates when sensitive data can be archived or otherwise removed.
- Where possible automate these redaction and archiving solutions so data retention becomes part of your normal business cycle – rather than project-based.
- Based on your retention policies undertake a cleanup and archiving project to remove, archive or redact data that you no longer have legal grounds to keep.



7. Manage SAP systems access risk, to restrict employee access to sensitive data.

- Determine where your sensitive and personal data is stored (transactions, table and associated business objects).
- Identify Roles and Users that have access to this data and develop rule sets and alerts so that access requests take cognisance of risks.
- Put in place a process to regularly review who has access to personal data.
- Clearly document the access policies and validation steps.



8. Encrypt data that leaves your SAP system.

- Implement encryption to prevent sensitive data from being stored at rest; any data stored on file servers or delivered through interfaces should be encrypted before transmission.
- Review your end-point security policy to ensure you have employed solutions that mitigate the risk of users who extract sensitive data through reporting, analytics, and knowledge-sharing with colleagues.



9. Review your audit tracking and logging maturity in SAP.

- SAP users extract hundreds of sensitive records and documents from SAP systems and applications for the purpose of reporting, analytics, and knowledge-sharing with colleagues, partners, and suppliers. Most enterprises have very little knowledge or control of where these documents are going, who accesses them, or how they are being used. This leaves companies at a high risk of data loss due to malicious or accidental actions.
- Simulate a data breach response and develop an action plan that outlines core responsibilities of all relevant role players (basis, network security, application owners, risk officers).



10. Define a solution compliance roadmap.

- Identify SAP solutions and processes to support: access risk, infrastructure security, risk assessment and internal controls, archiving, non-productive data management, breach notification and disclosure request management.