7 Practical Steps
to prepare your SAP systems for GDPR compliance

For most companies, GDPR (the General Data Protection Regulation) compliance is a huge project. There are a daunting number of systems and processes in the scope - particularly when organisations have invested heavily in broad SAP solutions (ECC, SRM, BW, CRM etc). Because of the nature and complexity of SAP solutions, sensitive data is stored and accessed in numerous techniques. This, compounded with high volumes, makes finding and managing the sensitive data a complex challenge.

Companies across the world are justifiably concerned about GDPR and how much they have to achieve by the deadline. In under a year – by 25 May 2018 – all organisations world-wide collecting, storing and processing personal data from European Union (EU) citizens must be ready to reveal the data they have on the individual and what purpose(s) it is being stored and used for.

Compliance will be non-negotiable - Organisations with data security breaches will face heavy fines, which could be as high as €20m, or 4% of annual revenue - whichever is greater.

Every organisation should be devising a plan to meet the requirements, and assigning key roles and responsibilities to that plan. To address this challenge and make it more manageable, EPI-USE Labs offers the following practical recommendations for those customers where SAP is the main system of record and a large part of the IT landscape.

Recommendation 1:
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.

Recommendation 2:
Reduce sensitive data on your non-productive SAP systems

- Reduce your risk profile by intelligently masking data in non-production systems. By taking your test systems out of the equation, they won't contain personal and sensitive data, hence reducing 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.

Recommendation 3:
Create processes for Access Requests and the Right to be Forgotten

- Develop a process and checklist for how your organisation will respond to information access requests. Design appropriate workflows and process flows, and assign responsibility to a specific team. This could include a customer-facing web solution to track and manage consent requests.
- Create a central mailbox or communication solution so that you can track regulator dialogues and interactions.

Recommendation 4:
Review your data retention policies to reduce historical data

- Review your data retention policies against the GDPR requirements.
- Develop an archiving 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.

Recommendation 5:
Manage SAP system 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 access to personal data.
- Clearly document the access policies and validation steps.

Recommendation 6:
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.

Recommendation 7:
Review your Audit tracking and Logging Maturity in SAP

- SAP users extract hundreds of sensitive 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).

How EPI-USE Labs can help

EPI-USE Labs offers a wide range of innovative add-on software and services to optimise SAP environments. These accelerate, automate and simplify data management with tangible benefits. We also offer state-of-the-art security solutions together with GDPR compliance know-how, to ensure peace of mind and business efficiency.

Data Secure (part of our Data Sync Manager (DSM) product suite) is a comprehensive protection solution that comes with predefined masking rules which mean you can scramble any non-key field in SAP. **Data Disclose** addresses compliance to the Right of Data Access by highlighting sensitive data across your SAP portfolio. To reactively address the Right to be Forgotten, **Data Redact** is a follow-on Fiori app from **Data Disclose** which intelligently removes data identified for redaction. **Data Retain** allows the company to proactively set up policies to address the Right to be Forgotten by removing data at predetermined periods.