EPI-USE LABS
value through innovation

MAKING COMPLIANCE WITH THE **NEW ZEALAND PRIVACY ACT 2020 EASIER**

[FROM AN SAP PERSPECTIVE]

A WHITE PAPER - Warren Eiserman

ARE YOU COMPLIANT WITH THE PRIVACY ACT 2020?

With GDPR in full force and reaching well beyond the European Union, data protection and privacy has become a priority for businesses all over the world. Starting in December 2020, organisations or agencies in New Zealand and elsewhere will also need to support the Privacy Act 2020 (the Act).

For those companies running SAP ERP, a number of approaches need to be considered to support the Act. It is likely that business processes, access control, code and infrastructure components will need to be re-engineered. Depending on the risk profile of your business, solutions can vary from lightweight interventions through to full security transformations for those in the defence, financial services, utilities or retail industries.

No single solution can address all aspects and complexities of the Act. The reality for most companies is that the Act isn't going to be a once-off exercise, but a journey in which capabilities will mature as businesses gets a better understanding of what works, and what may or may not be acceptable once the Act comes into force.

All businesses will need to review their processes and determine:

- the purpose for which data is being collected
- where the data is stored, how is it transmitted, and the associated audit records for the data, including stakeholders and role players
- who has access to the data
- how long data should be kept for, and what the processes are to remove data that is no longer required
- if all legal documents (employment contracts, privacy policies, consent forms, terms and conditions, electronic communication records, data processing agreements, supplier contracts etc) are compliant with the provisions in the Act.

HOW TECHNOLOGY SUPPORTS THE PRIVACY ACT 2020

The scope of this document is not to provide a legal background on the Act, but rather to highlight how technology can be an enabler for your compliance initiatives. Technology can support your efforts in the following broad areas:

DATA QUALITY (IPP 7 & IPP 8, SCHEDULE 9)

A broad range of SAP technologies supports the functions of creating, maintaining, archiving and distributing sensitive data across the enterprise. Master data maintenance and associated workflows ensure that personal data is captured and maintained appropriately.

DATA MINIMISATION (IPP 1 & IPP 10)

Ensures that your business keeps data that is required from a processing of compliance perspective and reducing the oversight and processes that are required. Minimisation applies to:

- Ensuring relevant data is captured (based on legal grounds)
- Limiting or obfuscating sensitive data in non-production systems
- Applying rules so that data is automatically archived, deleted or redacted

Request workflows and search technologies can be used to manage the process of requests and associated amendments and deletion requests.

LEGAL BASIS & CONSENT (IPP 1 & IPP 4, SCHEDULE 9)

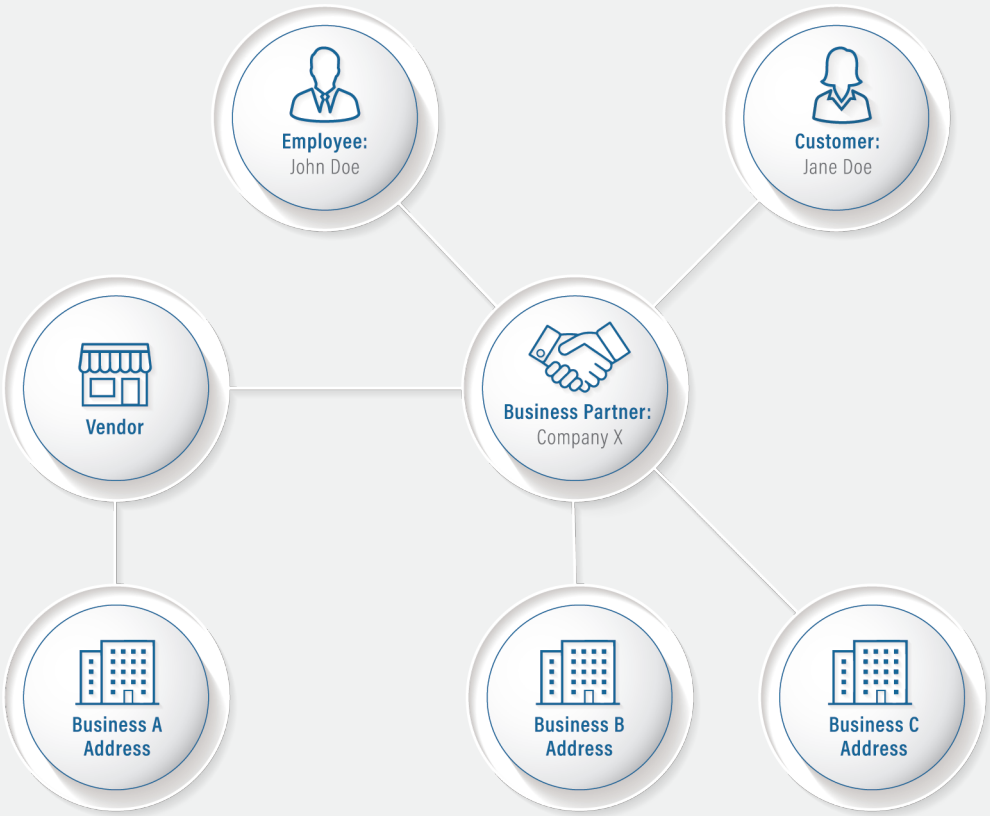
Personal information can only be used after obtaining consent from data subjects.
The associated tracking (and subsequent withdrawal) can easily be supported through technology solutions and associated workflows.

SECURITY SAFEGUARDS (IPP 5)

A broad range of technologies exists to prevent unauthorised access and interception of personal data. These include intrusion detection, encryption, monitoring, identity management and logging solutions. These cyber-risk technologies have the ability to detect or intelligently predict when sensitive data is being inappropriately accessed. The extent to which data protection is ensured depends on secure SAP system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance.

SAP ERP IN THE CONTEXT OF PERSONAL DATA

The integrated nature of an SAP ERP means that all your business data is connected and stored in complex data schemas within the SAP data model. SAP acts as a central nervous system that interacts with many other external systems through various interfaces.

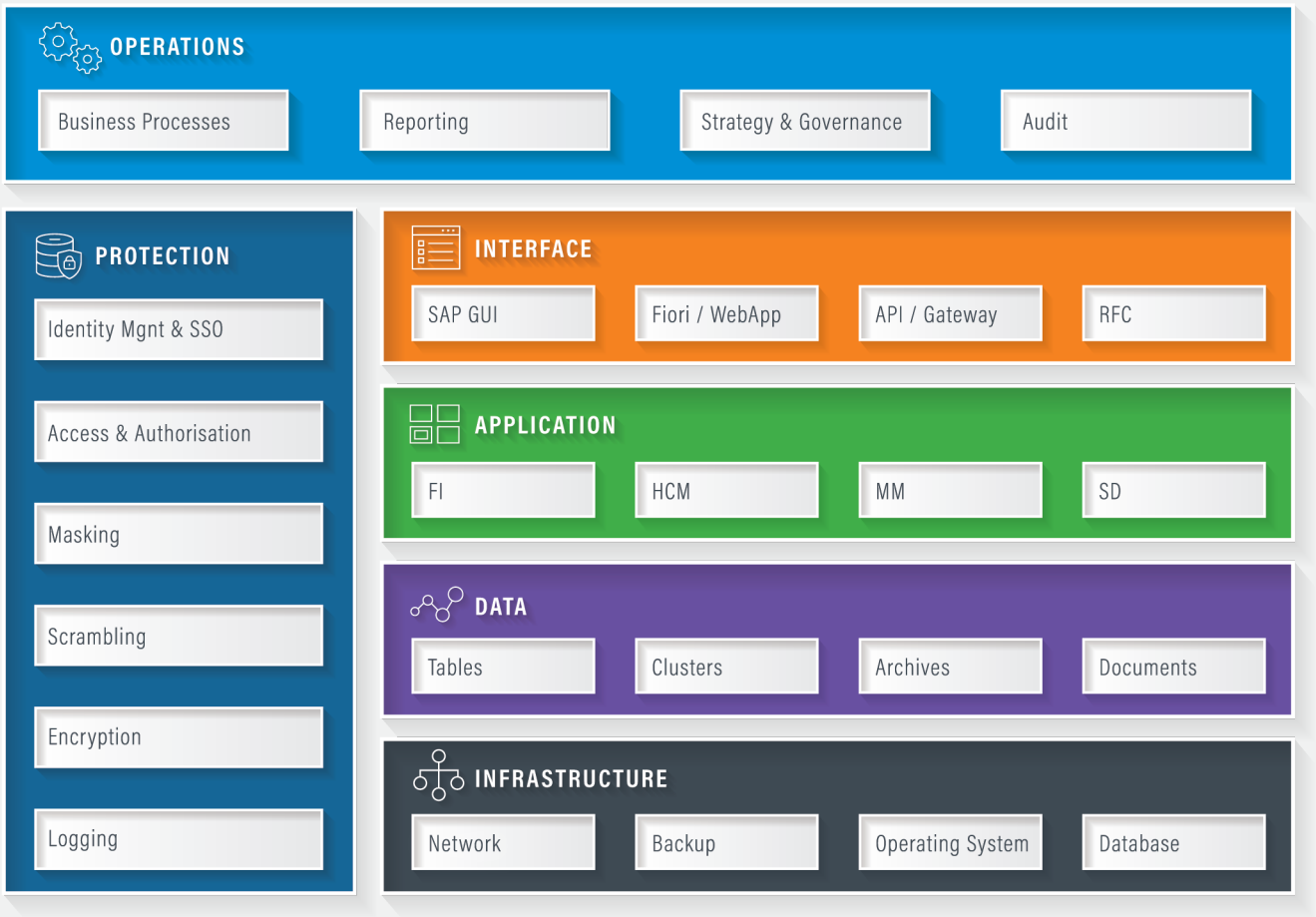


SAP introduces complexity for managing personal information, but there are also some advantages:

ADVANTAGES	CHALLENGES
Well-documented data model for personal data across customers, vendors, employees and business partners.	
Usually the primary data source for personal data, i.e. the "master", which feeds downstream systems.	Concept of "deletion" is not widely supported; original transactions and follow-on documents are processes requiring historic records.
Large customer base, ensuring there is pressure on SAP to deliver compliance and regulatory solutions 'out of the box'.	SAP cloud solutions such as SuccessFactors, Ariba, Concur and Cloud Integration make cross-system privacy processes more complex to manage.
SAP and third parties provide technology solutions to support risk and compliance processes.	Non-production systems require 'real world' data for testing, requiring secure copies of production or implementing a scrambling technology.
Audit firms have strong knowledge of the SAP environment, and offer proven methodologies for minimising risk.	SAP places the onus on the customer for customer data in non-production systems.

SAP SECURITY ARCHITECTURE LAYERS

When viewed from a privacy and security perspective, an SAP ERP consists of the following layers:



Another important aspect to consider in your application architecture: SAP systems are usually deployed in a three-tier landscape (DEV, QA and Production) which adds to the complexity of managing master data and transactions. Test and development systems shouldn't contain sensitive data, as they usually have more 'open' access for testing, development and configuration teams.

COMPLIANCE PROJECTS INVOLVING SAP GET COMPLICATED, FAST

A large portion of your compliance initiative will be setting up the strategy, roadmap and governance of your privacy program; this will dictate how you handle sensitive data within your IT environment. Your compliance initiative requires time and dedication from a broad spectrum of business departments, including HR Legal, Internal Audit, Sales and Marketing, Finance and IT.

Managing a complex, high-pressure project is a challenge, and like any challenge, it begins with a plan.

STARTING YOUR PRIVACY ACT 2020 COMPLIANCE PROJECT

Typically, compliance programs start with a Data Privacy Impact Assessment (DPIA) – a mechanism for determining people, processes and systems involved. By undertaking a DPIA, you will be able to identify the main business risks with respect to the rights of data subjects. You can then identify what the risk of processing incorrect or inaccurate personal data may be to your business. During the DPIA, you will identify those processes which interact with your SAP systems.

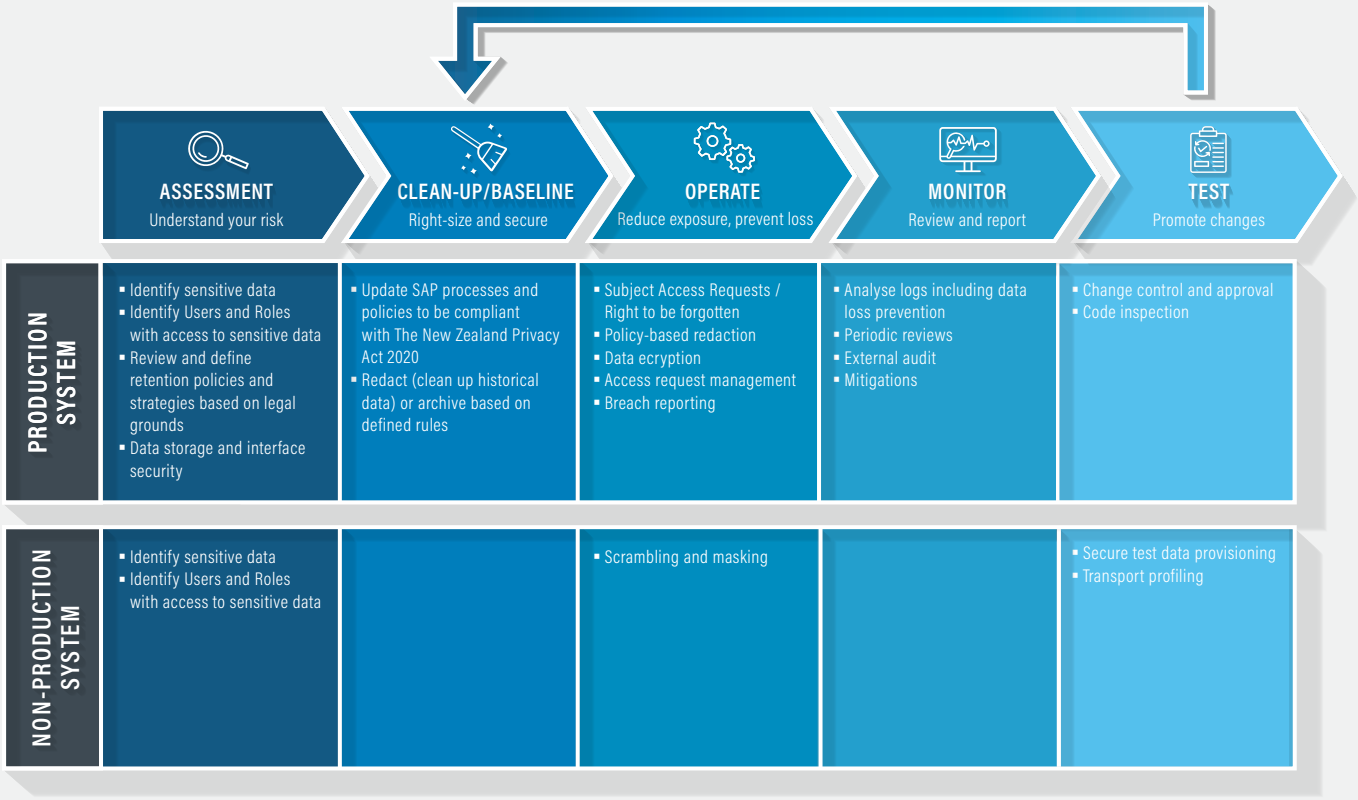
Steps involved in the DPIA include:

- **Plan**
  - Identify team and stakeholders
  - Define scope of assessment
- **Assess**
  - Track data flows across business process in scope
  - Review existing legal and privacy policies
  - Determine threats to privacy rights and business vulnerabilities
  - Determine controls and countermeasures
- **Implementation of Controls**
  - Follow data privacy guidelines
  - Determine privacy measures and responsibility matrix
  - Design or select security features
- **Sign off Report**
  - Define auditing procedures
  - Create follow-up activities

STEPS IN A TYPICAL SAP COMPLIANCE PROGRAMME

From an SAP system perspective, in our experience of implementing privacy solutions, programmes typically have the following components:

1. Assessment (component of the DPIA)
2. Clean up/Baseline
3. Operate
4. Monitor
5. Test



We distinguish between production and non-productive SAP operations as typically a significant amount of test data is needed to effectively test business changes through the landscape.

DATA PRIVACY IMPACT ASSESSMENT: RECRUITMENT SAMPLE

We have included some examples of a Data Privacy Impact Assessment (DPIA) that cover a typical recruitment scenario.

ASSESSMENT EXAMPLE

Below is an example of the type of questions that would be included in a recruitment process DPIA:

1. **Main HR Process**
    1. **Sub-Process Recruitment**
        i. Consent
            a. Has consent been built into candidate application and interview processes?
            b. Is explicit consent recorded? How is it been obtained (web, physical, verbal)?
            c. Can individuals withdraw consent? What is the process and length of consent on which we can retain information?
            d. Is it possible for individuals to restrict the purposes for which you process information?
        ii. Data Subject Participation
            a. Are processes available for handling data access and revision requests?
            b. How are third-party submissions handled for educational and criminal checks in the evaluation process?
            c. How are data deletion requests handled in the context of rejected applications?

iii. Data Minimisation
   a. What processes are in place to minimise data
      - During the CV and application process?
      - After successful placement?
      - For rejected candidates?
   b. How is testing handled in applicant tracking systems and core HR onboarding?
   c. What is an acceptable retention period for holding candidate data?
   d. Are processes in place to anonymise data (if required)?

iv. Third Parties
   a. Are data processing agreements in place with HR business partners and software providers (job boards, Linked-In, etc)?
   b. Are data processing agreements in place with other third parties?

v. Data Processing
   a. Are the company's data privacy policies included as part of the offer and contract process?
   b. Has a breach notification process been defined?
   c. Have all regulatory reporting requirements been considered in the context of data privacy? Ethnicity, religion, etc?

vi. Security Safeguards
   a. What security measures on integrity and confidentiality of candidate information have been put in place?

EXAMPLE ARCHIVING RULE SET

Below is an example of retention rules that could be defined to support the recruitment process.

SELECTION	RULES	ACTION	OUTPUT/VERIFICATION
Candidate	Candidate status is active; No pending hiring action; Not involved in any workflow	Redact candidate sensitive fields.	Candidate ageing report analysis. Redaction processing log review.
	Consent withdrawal. No other regulatory requirement exists to keep data	Redact all sensitive fields. Send redaction request to third parties (if required)	Redaction Workflow, Confirmation email.
Application	Unsuccessful applications older than 2 years	Delete applications and associated relevant non-successful applications	Report and log review.

TEN RECOMMENDATIONS FOR YOUR SAP COMPLIANCE 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.
   - 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 the Privacy Act 2020
   - 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 the Act, 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-productive 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**
   - Ensure you upgrade to the most compliant versions of SAP that are available; see SAP Note 1853572 for more information. This includes the latest security patches which are released on a regular basis.
   - 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 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 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 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.

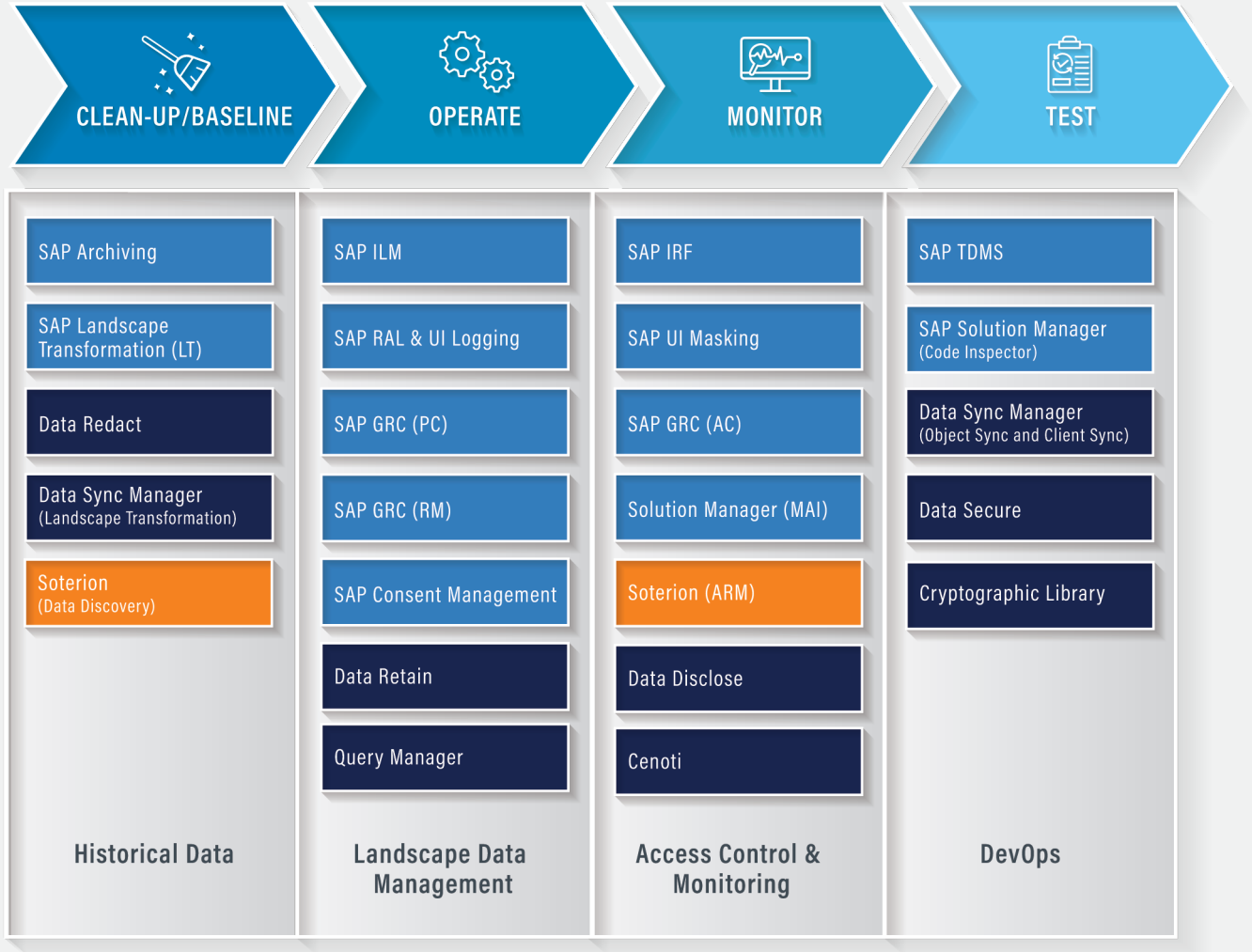
9. **Review your Audit tracking and logging maturity in SAP**
   - SAP users extract hundreds of sensitive documents from SAP systems and applications for the purpose of reporting, analytics, and knowledge-sharing with colleagues, partners, and suppliers. Most enterprises have very little knowledge or 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.

KEY AREAS TO FOCUS ON WITHIN AN SAP LANDSCAPE

The following are the key areas to focus on:

1. Historical data in your productive system
2. Process execution management
3. Automation of ongoing compliance activities to ensure relevant internal controls are being implemented effectively
4. Managing sensitive data in your DevOps processes e.g. PII data in non-productive systems
5. Consent and legal basis management including customer requests



TECHNOLOGY ENABLERS

A number of technology enablers exist to support customers, both from SAP and third-party providers. We have highlighted the major solution offerings below, but this is not an exhaustive list.

SAP SOLUTIONS

EMBEDDED CAPABILITIES

Within the core SAP business systems such as ERP, a number of approaches are possible:

- Configuration to adjust business processes
- Roles and authorisations
- SAP Business Workflow solutions
- Custom ABAP solutions, reports and logging
- Archiving

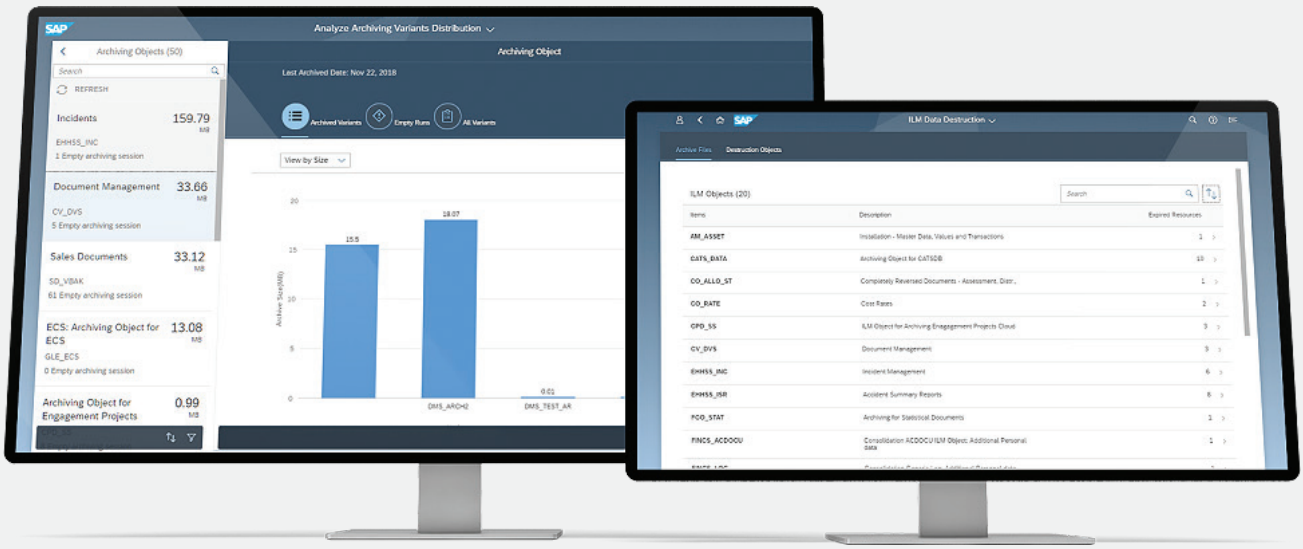
SAP INFORMATION LIFECYCLE MANAGER

A solution to manage the lifecycle of your business data based on a set of rules, which are broken into two broad categories:

- **Residence rules** describe the period for which you would like to keep business-related data before archiving it, also called end of business (EoB)
- **Retention rules** describe how long you should be "keeping" the business-related data overall, also called end of purpose (EoP)

SAP ILM is purchased separately from your ERP system and leverages classic data archiving functionality within SAP. The solution includes a 'blocking mechanism' for viewing of data, and provides a set of configuration and access control capabilities.

From Netweaver 7.5 onwards, it is also possible to implement a data controller rule framework to assist in the definition of rules to support multiple retention requirements (such as GDPR). ILM also makes use of the Information Retrieval Framework (IRF), a separate business function to perform the information indexing.



SAP READ ACCESS LOGGING

Read Access Logging (RAL) monitors users' activity in your SAP system and provides an audit trail of access. RAL allows you to track:

- who had access to the data
- which data was accessed
- when the data was accessed
- the mechanism that was used to access (transaction or user interface)

The RAL configuration approach is to tag fields and tables (including custom ones) which contain sensitive data. Once activated, interrogation of the log is possible to monitor activities. Alerting is implemented using the Monitoring and Alerting Infrastructure (MAI) of SAP solution manager and can be configured to send email alerts to your internal audit team based on specific criteria.

The solution allows configuration of reason (Logging purpose) and areas (Logging Domains) that you wish to activate logs for. This allows specific content to be logged for auditing purposes and provides you with detailed logs should you need to review who has accessed personal information. Default logging configurations are available per SAP application (see SAP note 2347271).

SAP UI masking functionality ensures that personal data is masked when viewing data via GUI, Web Dynpro or Fiori applications. Authorised users (with display rights) can display blocked data; however, they cannot create, change, copy or perform follow-up activities on blocked data. Masking configurations are based on existing Read Access Logging (RAL) configurations.

An additional product called UI Logging is also available, which can be used to detect and act on misuse of legally protected or business critical data. This is commonly used with an SAP cyber security product called Enterprise Threat Detection (ETD).

SAP INFORMATION RETRIEVAL FRAMEWORK (IRF)

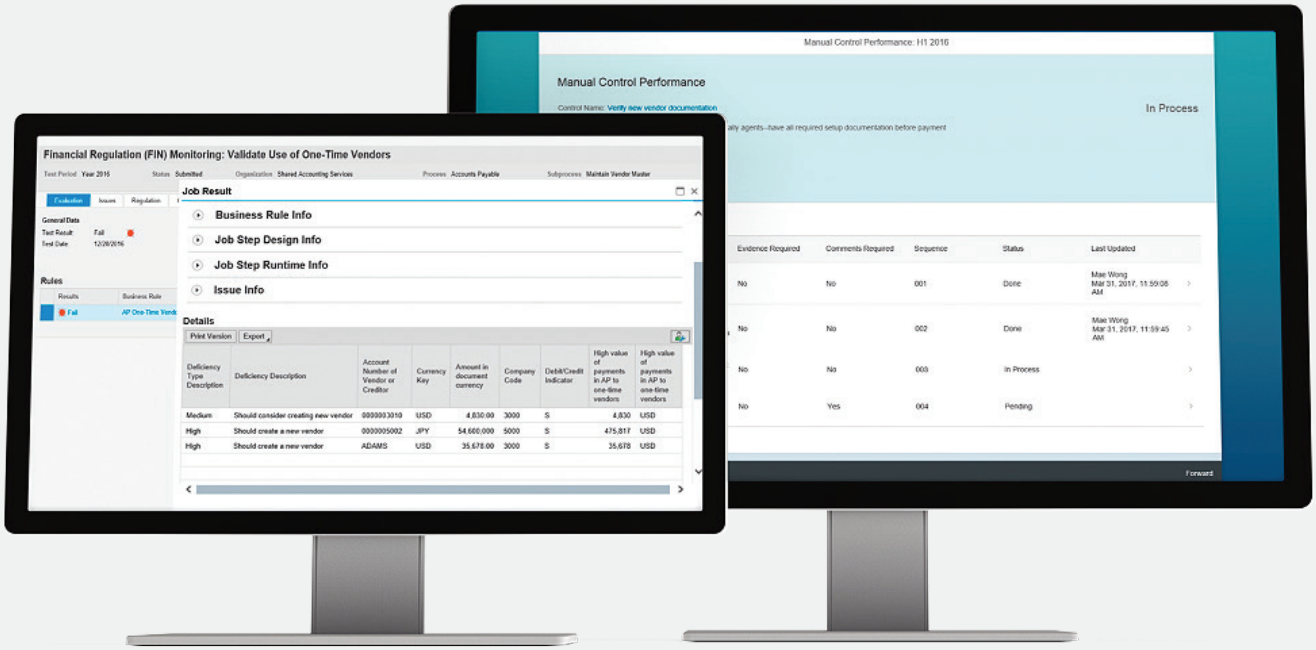
This offers a search and retrieval solution for personal data of a specified data subject. This function is carried out in all systems which have the business function active. Search results return a list containing personal data of the data subject specified, subdivided according to the purpose for which the data was collected and processed.

To be able to use the retrieval functionality, you must create your own data model as a basis for the retrieval process.

SAP GOVERNANCE RISK & COMPLIANCE (GRC)

GRC can leverage information within your existing business applications so you can evaluate risk and apply controls directly within business processes. These sub-modules work together to automate end-to-end GRC activities, including corporate governance and oversight; risk management; control testing and remediation case management; user access and authorisation. The solutions support the following business-critical functions:

- Central management of GRC information in a single system of record, including corporate policies, regulations, compliance and control frameworks, business process flows, and risk and control libraries
- Proactive identification, analysis, and monitoring to forecast and respond to potential threats
- Automated controls to ensure appropriate user access and authorisation
- Monitoring of business processes to promote desired behaviours and maximise results



Risk Management (RM)

GRC (RM) equips managers to properly analyse risk-reward trade-offs and carry out appropriate responses that are backed by quantitative metrics. The solution enables enterprises to implement proactive, collaborative processes to balance opportunities with financial, legal, and operational risks at all levels of the enterprise. The software provides a best-practice framework for enterprise risk identification, collaborative risk analysis, predefined risk responses, and continuous risk monitoring and reporting so that you can effectively anticipate and respond to changing business conditions. Key risk indicators enable you to monitor the overall risk portfolio and to alert management immediately when high-impact and high-probability risks exceed company specific thresholds.

Access Control (AC)

GRC (AC) allows implementation of comprehensive risk based access and authorisations across your organisation. Access Risk Analysis tool allows identification, analysis and resolution of access risks. An expandable set of rules is used to detect conflicting access or who has access to personal information. Rulesets are developed to control which users have access to personal information.

Process Control (PC)

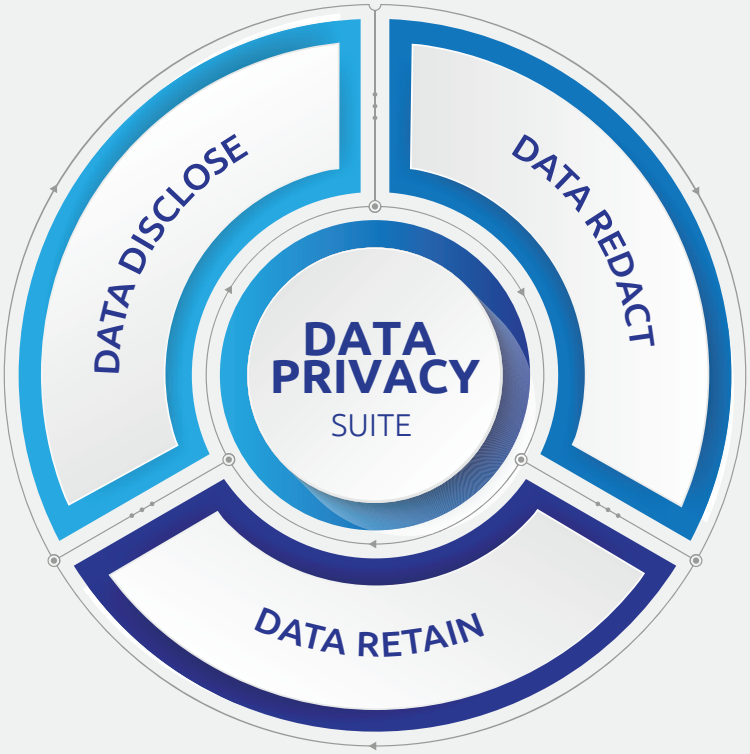
GRC (PC) applies a risk-based approach to setting up your control environment and identifying the most effective and efficient controls needed to achieve compliance to any legislation. The application integrates directly with control documentation in SAP GRC Repository, enabling you to centralise control management and to eliminate the need to integrate separate tools for documentation, testing, remediation, and control monitoring. The solution allows the monitoring of hundreds of critical processes: procure-to-pay, order-to-cash, hire-to-retire and IT controls. A single automated control test for multiple combinations of criteria, such as data subject de-identification ensures compliance. The manual control test is routed to the appropriate person for timely performance and guides the tester with step-by-step procedures and approved templates to minimise errors. Additional survey functionality allows self-assessment for entity-level controls and management sign-off.

Provides support for:

- Governance and Policies
- Assessments and surveys (incl. Data Privacy Impact Assessments)
- Assurance and reporting

GRC also can be integrated with the SAP ILM solution to assign ILM objects to audit areas (if required).

THIRD-PARTY SOLUTIONS



EPI-USE LABS' DATA PRIVACY SUITE[14]

Our data privacy and compliance solution helps companies with SAP systems efficiently address compliance with the Privacy Act 2020, with pre-built solutions to key technical and process challenges. It is composed of three key solutions:

DATA DISCLOSE™

Data Disclose is an application that enables you to search all SAP systems used by your organisation to find where personal data is stored. Typically, one data subject's record exists in several development, test and production systems. You may also have external systems that connect to a SAP environment which contain some parts of the data. For those systems, you can use our APIs to connect (or use our consulting team to connect) them to Data Disclose. It means one place to search, review and present the entire footprint for a data subject.

DATA REDACT™

Data subjects have the Right to Erasure (Right to be Forgotten); the right to have personal data erased and to prevent processing in some specific circumstances. Data Redact allows you to remove the sensitive or identifying data without removing the entire record. This makes the process simpler and less invasive. The data is effectively submitted for redaction so the data cannot be identified.

DATA RETAIN™

This application will allow an organisation to build highly configurable rules which can apply retention periods to different types of data. When executed, it will apply those rules to identify sets of data which are now due for redaction. This will allow you to keep applying retention policies and redacting data yourself beyond the duration of this project.

EPI-USE LABS' DATA SYNC MANAGER™ (DSM) SUITE[15]

DSM can rapidly create new non-production systems, reduce the footprint when refreshing existing test clients or creating new ones, and copy selected data on demand, all with integrated scrambling of data for security.

DATA SECURE™

Data Secure is a data-protection solution that masks SAP data to safeguard sensitive information, either in-place for non-productive clients, or 'at source' .

CLIENT SYNC™

Client Sync allows you to copy only the subsets of information you need from a production system. This has impressive advantages: it reduces the new client's footprint and saves valuable disk space – up to 90%; which means your costs and copying time are drastically reduced, all without interrupting the landscape.

QUERY MANAGER™

Query Manager allows business users to identify and report on sensitive HCM and payroll data securely. It includes the ability to encrypt and password protect reports which contain sensitive and personal information.

DOCUMENT BUILDER™

Document Builder helps you create richly formatted letters, documents, reports and visualisations for automated distribution to employees, managers and business partners, including ability to: encrypt, password protect or include digital signature capability - protecting report data "at rest".

TAKE PRACTICAL STEPS NOW

The requirements for the Privacy Act 2020 can be daunting, but if you work closely with your audit and legal teams and remain pragmatic, there are a number of effective steps you can take depending on your risk profile. The bulk of your activities will be around reviewing your business processes and associated compliance framework.

Leveraging technology enablers will accelerate your journey to compliance, and demonstrate that you have taken steps to support the legislation.

NOTES AND REFERENCES

1. Clean your SAP data and reduce risk:
   https://www.epiuselabs.com/asset-delivery-gdpr-data-removal
2. SAP Information Retrieval Framework (IRF):
   https://help.sap.com/viewer/1b0aa06133bd47ce8843635a99ee8ef5/7.51.5/en-US/b7ce5c62b41947adbf034900bd7eb084.html
3. SAP UI Masking & Logging solution:
   https://www.sap.com/documents/2015/06/0a0d918e-5b7c-0010-82c7-eda71af511fa.html
4. EPI-USE Labs' Data Privacy Suite: https://www.epiuselabs.com/data-privacy-gdpr-suite
5. EPI-USE Labs' Data Secure: https://www.epiuselabs.com/data-secure
6. EPI-USE Labs' Query Manager: https://www.epiuselabs.com/qm
7. Key changes in the Privacy Act 2020:
   https://www.privacy.org.nz/blog/key-changes-in-the-privacy-act-2020/