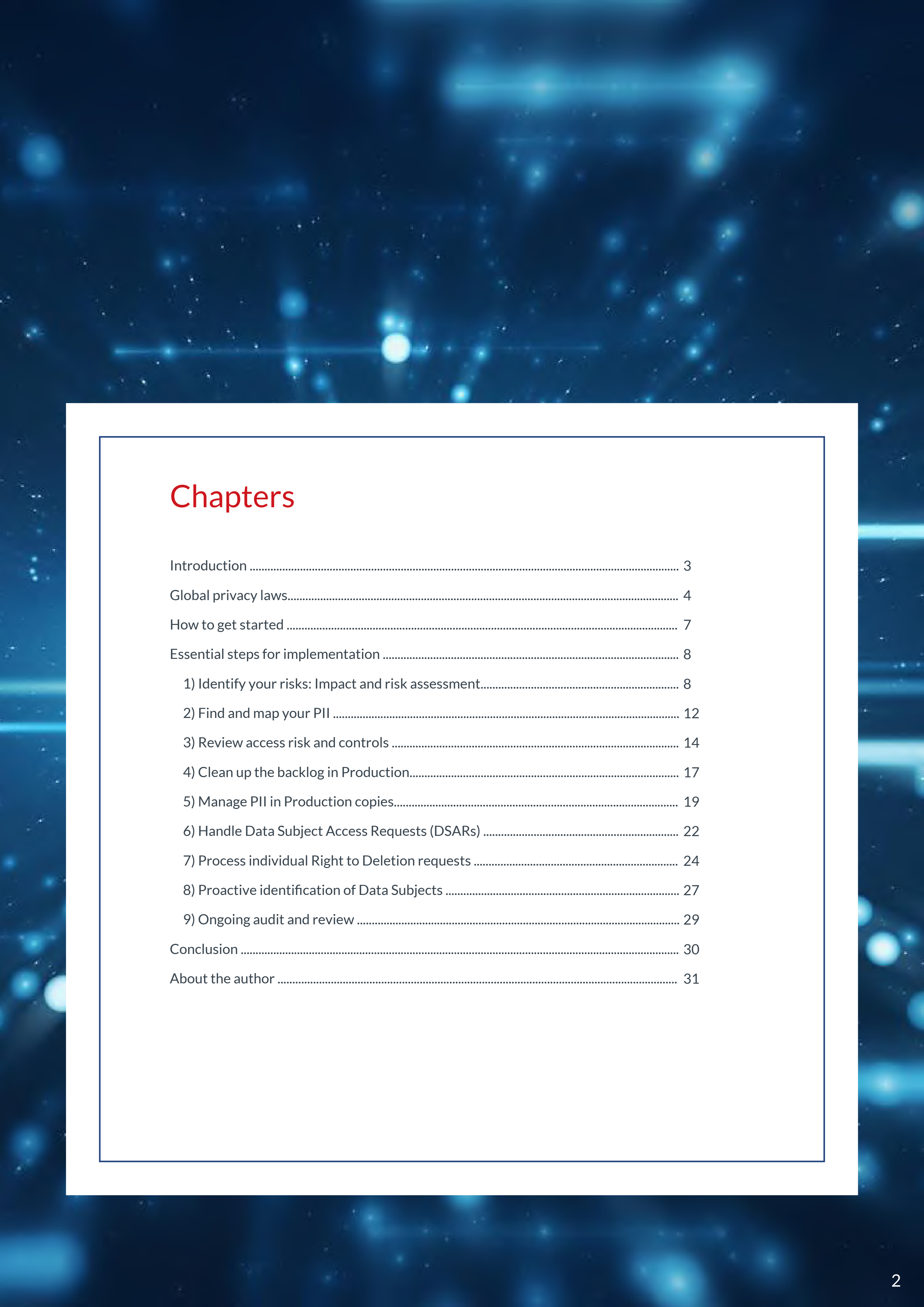
ebook:

Road to SAP data privacy compliance:

A practical guide of essential steps for data privacy compliance in SAP, based on lessons learnt from global data privacy projects

James Watson | Line of Business Owner
Privacy, Risk and Industry Solutions at EPI-USE Labs

James is responsible for the global line of business for EPI-USE Labs' data privacy and SAP IS-* Solutions, supporting all regions and key accounts running Data Sync Manager (DSM) for these complex requirements. With a functional and business background of over 20 years, James provides the bridge between Development, Basis, Test/Competency Centres and leadership teams to provide guidance and advise on the route to data privacy compliance. His history includes SAP specialisms in non-production data management and anonymisation, Production data removal or redactions, System Landscape Optimisation (SLO) and SAP industry solutions.



Chapters

Introduction

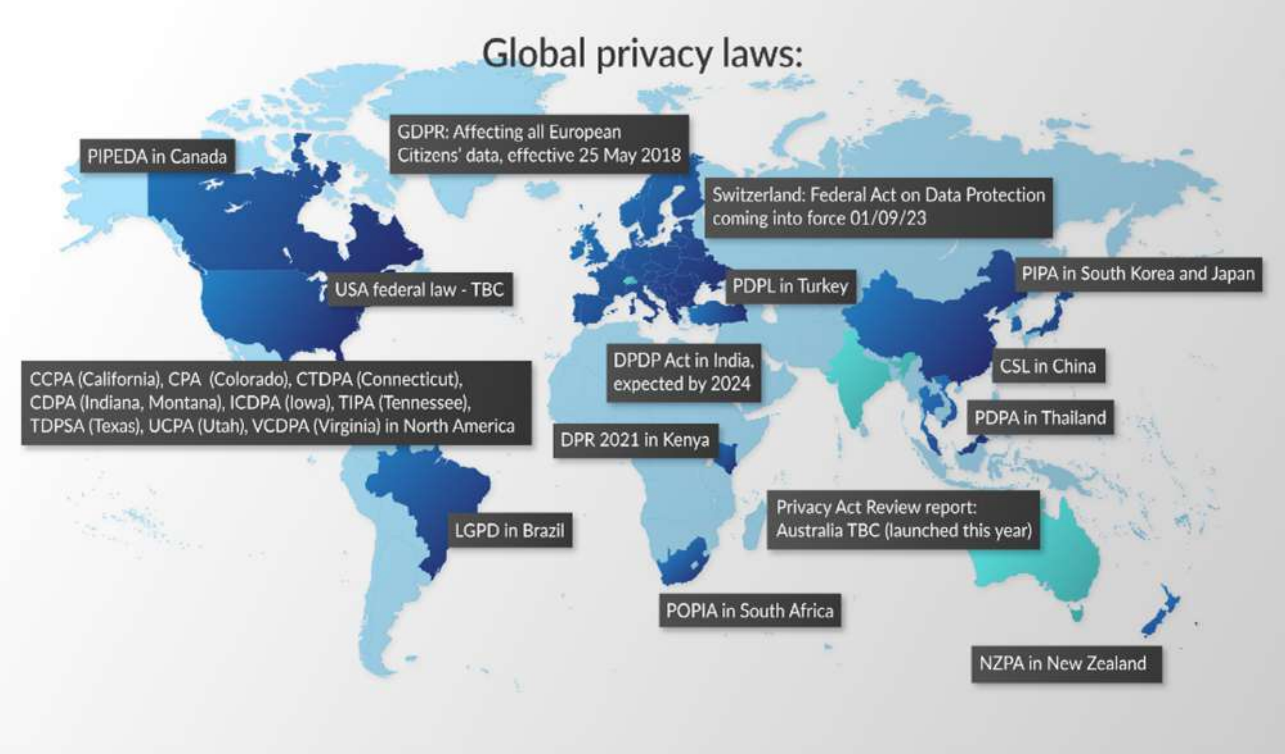
SAP is one of the most robust systems in the world, but also one of the most complex. SAP's structure makes addressing data privacy compliance particularly tricky. Detailed domain knowledge is required to map and understand the cross-functional integration of multiple SAP objects and systems.

EPI-USE Labs has been an SAP partner for over 30 years, and has an in-depth understanding of how SAP data is structured. We have worked closely with companies around the world, helping them to become compliant with global data privacy legislation such as the GDPR (General Data Protection Regulation).

This ebook is a practical guide outlining essential steps in the implementation approach for data privacy compliance in SAP systems, based on lessons learnt from various complex projects. I have focused on my particular experience in SAP; although the process principles will remain the same for different applications, such as Microsoft Dynamics and Oracle, the underlying technology will differ.

I hope this will give you some insights when you start your journey to data privacy compliance.

Global privacy laws


Global privacy laws:
PIPEDA in Canada
GDPR: Affecting all European Citizens' data, effective 25 May 2018
Switzerland: Federal Act on Data Protection coming into force 01/09/23
USA federal law - TBC
PDPL in Turkey
PIPA in South Korea and Japan
CCPA (California), CPA (Colorado), CTDPA (Connecticut), CDPA (Indiana, Montana), ICDPA (Iowa), TIPA (Tennessee), TDPSA (Texas), UCPA (Utah), VCDPA (Virginia) in North America
DPDP Act in India, expected by 2024
CSL in China
PDPA in Thailand
DPR 2021 in Kenya
Privacy Act Review report: Australia TBC (launched this year)
LGPD in Brazil
POPIA in South Africa
NZPA in New Zealand

As of October 2023, there have been around 20 revised privacy laws which have been enacted throughout the globe:

- GDPR in Europe
- CCPA (California)
- CPA (Colorado)
- CTDPA (Connecticut)
- CDPA (Indiana and Montana)
- ICDPA (Iowa)
- TIPA (Tennessee)
- TDPSA (Texas)
- UCPA (Utah)
- VCDPA (Virginia)
- POPIA in South Africa
- PDPA in Thailand
- LGPD in Brazil
- PIPA in South Korea and Japan
- NZPA in New Zealand
- PIPEDA in Canada

Also currently in proactive review is the DPDP Act in India, and the Federal Act on Data Protection in Switzerland is nearly passed. Federal laws to cover Canada, USA and Australia continue to be debated and are probably inevitable.

Each law is distinct, and contains its own intricacies; however, general themes for consideration in the digital world include big data, individual privacy rights and accountability. One of the most important is the focus on the individual's sovereignty, rather than on the data storage location; for example, a European citizen is covered by the GDPR when doing business or being employed anywhere in the world.

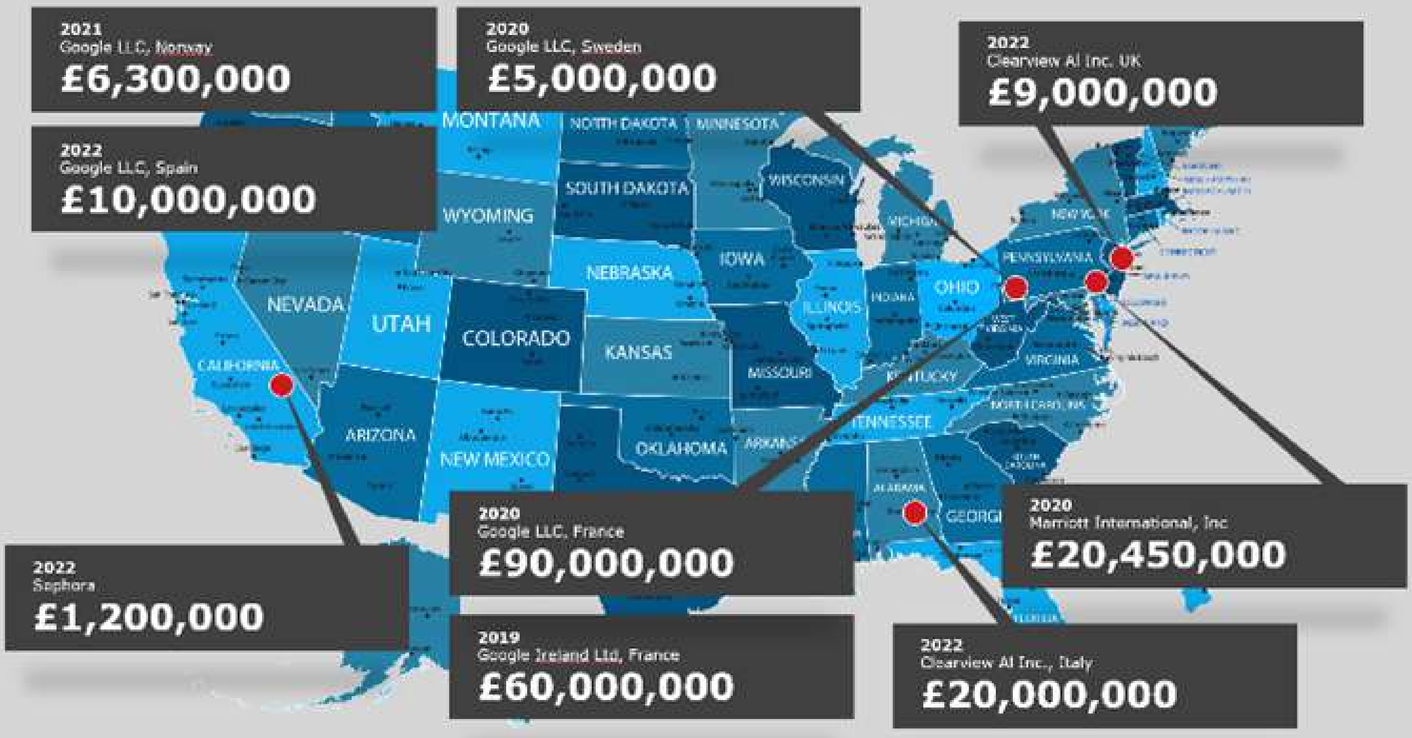
This does of course generate some interesting international law questions, but I am going to steer away from these legal concepts, and focus on the practicalities for an IT team when adapting processes and creating retention periods for data within a living Production landscape.

I've given a quick overview below of some of the core tenets which apply to each of these laws.

Privacy item	Explanation
Accountability	Every company is initially responsible for appointing a Data Protection Officer who is ultimately legally responsible for privacy within their business. In addition, clear definitions of Data Processors are made, keeping accountability within each company for the data they accept from other sources or move on to other related businesses.
Right to Access	This is often referred to as a Subject Access Request (SAR or DSAR). It requires any Data Processor to be able to search and identify a Data Subject within their business estate, and provide a summary of all Personally Identifiable Information (PII) held for them. A comprehensive report must be produced within a fixed period; some differences exist between the laws, but generally 28 days / 1 month is referenced.
Right to Deletion	A key addition to many of the privacy laws is the Right to be Forgotten or Right to Correction/Deletion. Here the onus of proving a legal justification for the PII data held within a business falls on the business; if no justification can be made, then every Data Subject has the right to request it is removed. From a technical viewpoint, the definition of 'deletion' is not explicit, and this is therefore open to your legal team's review. However, deletion is a challenge in many Relational database types. In this document, I will explore the options available and my recommendations.
Right to Portability	This is similar to the Right to Access. However, as opposed to the Subject Access Request, this defines the need to be able to extract all personal information to be shared between businesses at the request of a Data Subject. As such, this data must be in a common readable format that can be processed by different businesses. Although not explicit in some of the laws, there is an additional requirement to have sufficient checks and procedures around such a file-share to protect the individual.
Proactive privacy management	An essential item for consideration by all businesses, this enforces the need to create retention policies for your data, including proactively identifying Data Subjects (and their related data) where organisations no longer have the legal justification to maintain that information, and processing data removal.
Cross-border data access	Often referred to under the banner of Schrems II (although this is specific for EU -US data transfer) this deals with the scenario of sharing data between legal jurisdictions. A simple scenario we often come across is employee data which is being managed centrally in one office for a multinational business. These articles define allowable data transfer. This can raise a particular challenge, as businesses want the advantage of a single HR and Payroll technical solution, but then also need to ensure that only relevant users can access specific datasets.

There are more areas of commonality in privacy laws; however, for the purposes of this document, these are the main areas I have focused on.

One of the most compelling reasons for data privacy compliance is the enforcement fines; the new laws provide for far higher financial sanctions to be applied by the legal bodies, as in the examples shown below.



2021
Google LLC, Norway
£6,300,000

2020
Google LLC, Sweden
£5,000,000

2022
Clearview AI Inc. UK
£9,000,000

2022
Google LLC, Spain
£10,000,000

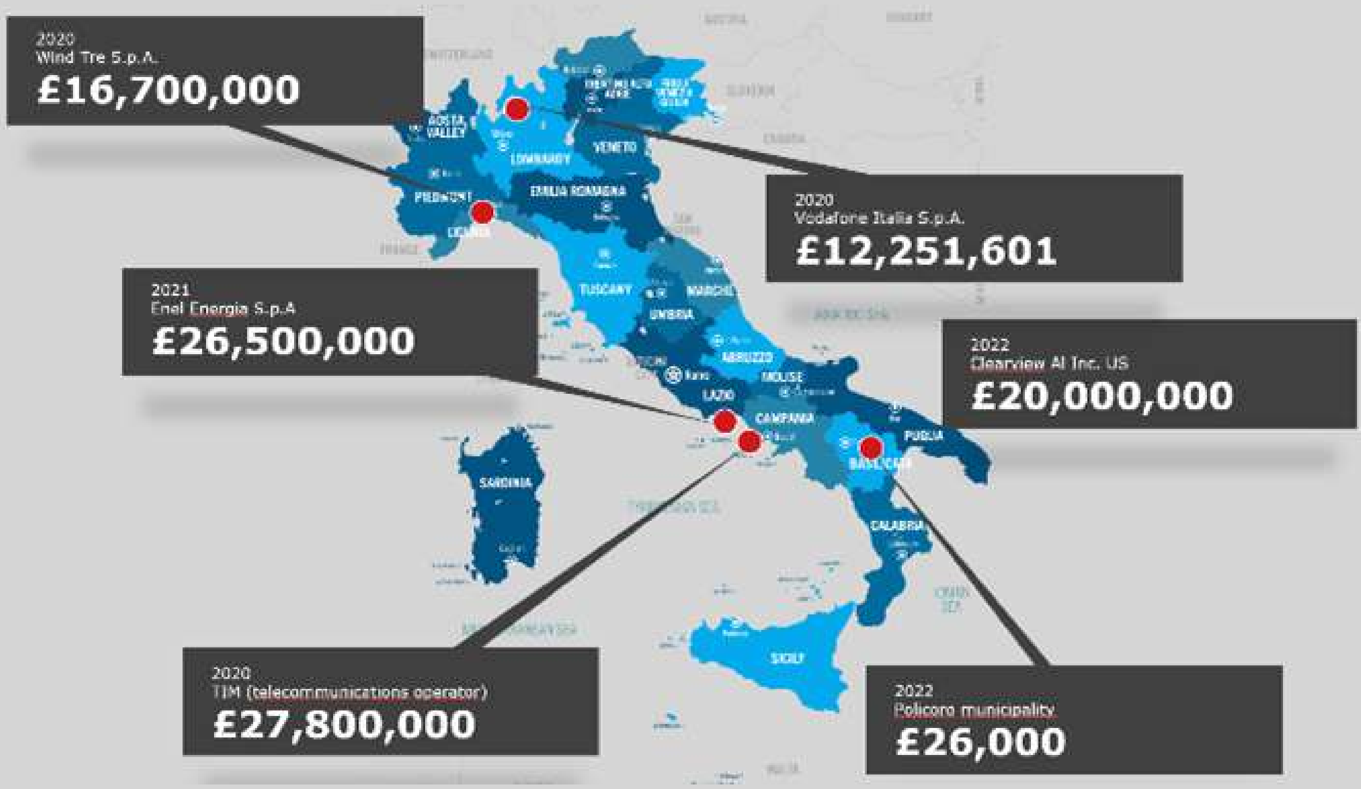
2022
Sephora
£1,200,000

2020
Google LLC. France
£90,000,000

2020
Marriott International, Inc
£20,450,000

2019
Google Ireland Ltd, France
£60,000,000

2022
Clearview AI Inc., Italy
£20,000,000



2020
Wind Tre S.p.A.
£16,700,000

2020
Vodafone Italia S.p.A.
£12,251,601

2021
Enel Energia S.p.A
£26,500,000

2022
Clearview AI Inc. US
£20,000,000

2020
TIM (telecommunications operator)
£27,800,000

2022
Policoro municipality
£26,000

How to get started

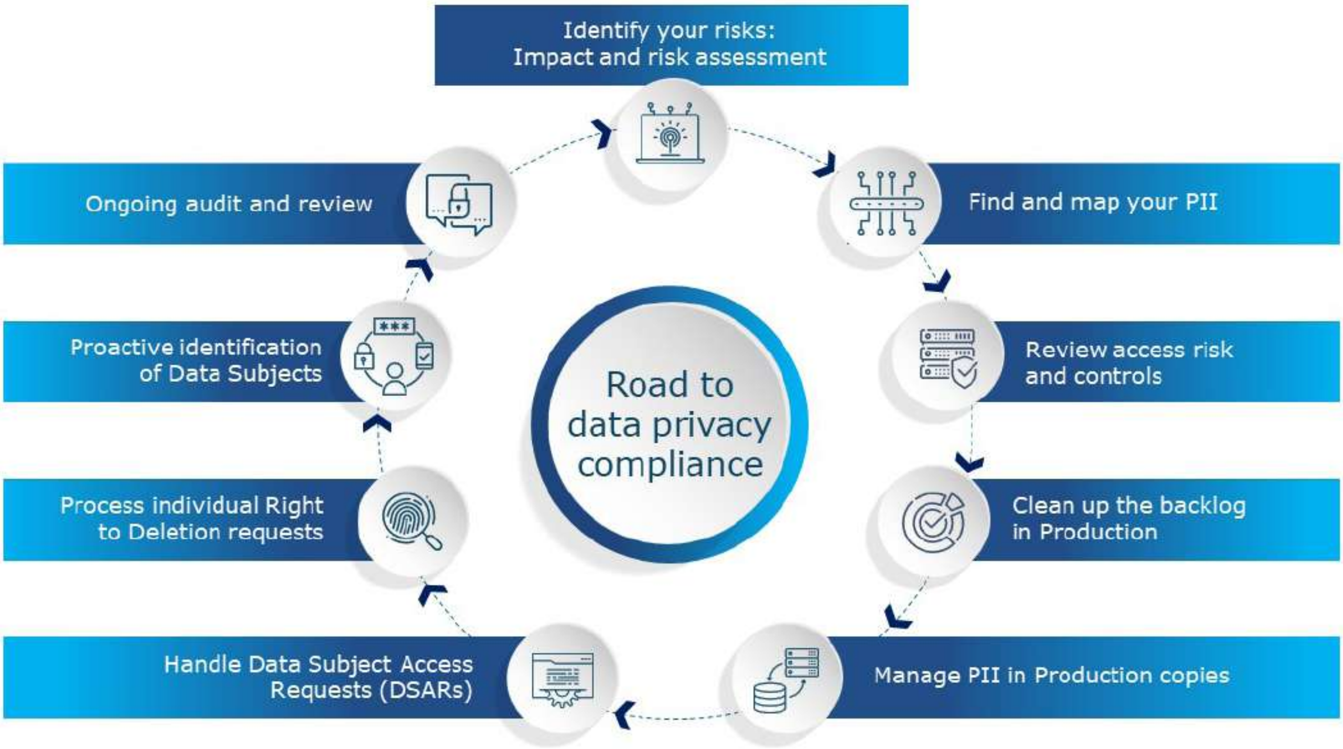
Every business is different and will have their own unique challenges; there is no ‘silver bullet’ which will solve all your data privacy challenges.

I’d suggest being careful of any company offering ‘out of the box compliance’; there are some great accelerators on the market, but any processes always need to be implemented and customised to your specific business.

This point is of even greater importance when reviewing technical solutions for SAP. For example, there are providers claiming AI and Machine Learning (ML) solutions which can automatically identify PII in your environment.
While pattern-matching ML may be able to find table fields where data is mapped, it can’t understand the referential integrity of the SAP database. At best, this will mean that data scrambling or removal won’t be consistent or complete; at worst, this will break the SAP system by creating missing data in the referential chain. As such, when reviewing solution options, I would recommend selecting specialist providers with available references in similar industries and system types to the systems you are running.

Having said that, the actual implementation approach can be standardised into a few essential steps, no matter the technology or industry. What you do in each step will be very different depending on your situation. At EPI-USE Labs, we call this ‘the road to data privacy compliance’. In this document, I explore each of these steps in more detail.

A final thought: don’t underestimate the importance of a solid requirements gathering phase, with clear scope for all involved. You will undoubtedly have unforeseen impacts and changes to manage by implementing software which will effectively delete data from your Production system. This can become very costly and extend your timelines. If you include as many decision-makers as possible in the blueprint of the project, and get sign-off for the delivery upfront, this will ease your route to going live.


Identify your risks:
Impact and risk assessment
Find and map your PII
Review access risk and controls
Clean up the backlog in Production
Manage PII in Production copies
Handle Data Subject Access Requests (DSARs)
Process individual Right to Deletion requests
Proactive identification of Data Subjects
Ongoing audit and review
Road to data privacy compliance

Essential steps for implementation

1) Identify your risks: Impact and risk assessment

Getting this and the next step right are what will set you up for success moving forward.

Risks outside of IT?

Before I focus on the technical IT assessment requirement, remember that the privacy project will not be solely focused on IT, but also needs to consider the people and business process elements of running your company.
For example, two common scenarios I have seen at multiple clients:

Scenario 1
Front office staff dealing with customers

When I worked in a contact centre many years ago, I would regularly use a notepad to record pertinent details of calls taken, marking down identifiers, accounts numbers, telephone numbers (in case the call drops), etc.; keeping the call short and completing the admin of entering this data after the call.

I would then regularly put the notepad in my bag at the end of shift, and take the bus home. What would have happened if I left that notepad on the bus?

What if I used a laptop? As we've seen many times in the news, laptops left in public places then result in data breaches.

The overall data privacy and security process needs to consider confidential waste disposal, VPN/MFA devices and more.

Scenario 2
Visiting an office

When I visit our client sites, I will regularly have an image taken of myself for an access badge, and might be requested for proof of ID, which will be copied and stored. What is the legally justified period to keep these records?

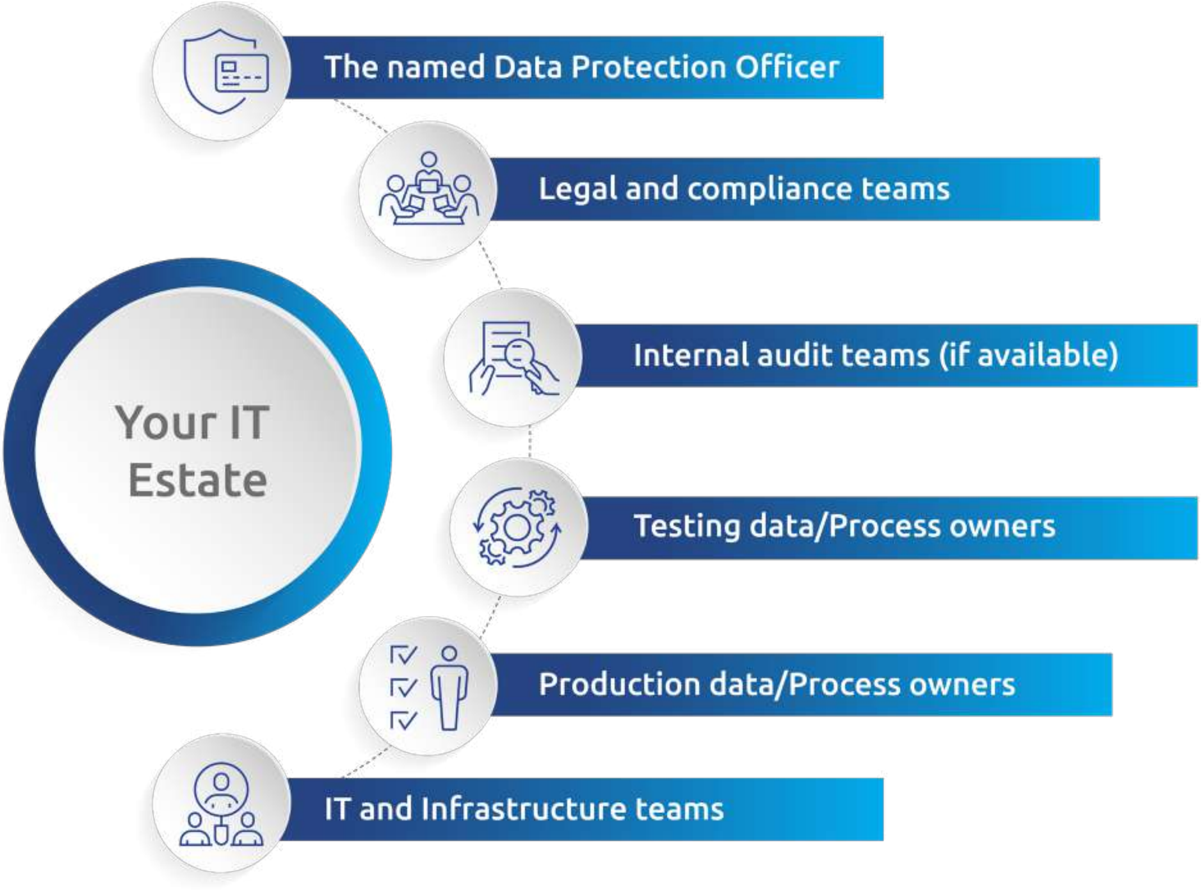
My least favourite is the very common site sign-in book, an open register which anyone can access, in which every person visiting is requested to enter their name, company, car registration and contact telephone number. The whole book could be stolen, or images taken of different pages, causing a breach under the privacy laws.

Of course, each company would need to keep a record for a period of time in case of incident. However, could a paper book be replaced with digital sign-in? Can retention periods be set against this data?

It is often actually easier to define and control the IT estate within the bounds of the privacy laws, and it should be a primary focus. But it's important for all privacy professionals to realise that you can't focus only on fixing IT systems and be compliant with the legislation.

Your IT estate: participants in this phase

Regarding the IT estate, the best run projects I have seen have involved these participants in this phase:


Your IT Estate
The named Data Protection Officer
Legal and compliance teams
Internal audit teams (if available)
Testing data/Process owners
Production data/Process owners
IT and Infrastructure teams

The **Data Protection Officer (DPO)** is essential to solve stalemate situations between the business and compliance. The officer should have the seniority to be able to make these decisions when needed. I have seen projects where the blueprint phase was less successful, and our client's 'lesson learnt' after the project identified the need to have the DPO involved early, to enforce the need for data anonymisation. Functional teams in general will not want to remove any data 'just in case' the customer was to return.

Legal and compliance teams have two key activities during this phase. The first is to give input on the privacy laws which the different parts of the business will be subject too. Of equal importance is the view on other regulations that impact the privacy laws. A common example is Taxation laws, which have strict guidelines on the length of time for which businesses are required to keep records from financial transactions. Understanding these additional compliance and legal requirements will drive the identification of your data retention framework.

Audit teams are a valuable addition; they understand what they would be checking under an audit to provide sign-off. Involving them early can avoid costly project upsets later down the line.

Testing owners are pivotal. Every business running SAP has copies of Production data provided to be able to test process changes, system updates or new functionalities before impacting the Production system. The process is essential for every business. As most businesses have gathered both informed and explicit consent to use their employee, customer and supplier data for testing, this now needs to be carefully managed. A clear understanding of the impacts of data scrambling will be needed to develop a design which is both compliant and has the least impact.

Similarly, the **Production process owners** will need to advise on the impacts of data removal to be compliant. Sometimes this creates a business justification which the legal and compliance team can argue into the company retention design. Alternatively, there may be process changes which need to be managed to meet the compliance requirements, and these owners will be responsible for moving these forward concurrently with the technical solutions implementation.

The **IT and Infrastructure team's** role during this stage is to advise of data transfer via interface between systems and key integrations. For example, where an email address is used in the interface to a web client solution, what are the technical options to continue to test this process but without 'real' email addresses? They will also give guidance into how data is transferred: is it pushed from one system or pulled from the other? This can define the complexity of the required solution. Where data is pulled from the single system of record to secondary systems, you only need to update the "master" system and these change will inherit to integrated systems. Whereas if it is pushed, a new job or interface to trigger updates may be required to achieve the same effect, which increases complexity.

Priority and level of risk

One of the best outputs for the technical analysis I’ve seen was laid out as a system architecture map with ‘traffic lights’ to show the priority and level of risk:

- Red indicates a high-risk system requiring direct processing. The system contains sensitive PII which is processed directly, not inherited from any other system, and has no delivered privacy functionality. This is a Priority 1 instance for the Privacy project.

- Amber indicates a medium-risk system. The system either:
- 1. Contains limited sensitive PII
- 2. Has an existing API function which will inherit anonymisation
- 3. Has in-built privacy solutions as standard.
- This is identified as Priority 2, requiring review but with a plan.

- Green indicates a low-risk system. This is reserved for systems where no PII is processed, only business data, and as such no review is required.

With this landscape view, you are ready to prioritise and identify the vendors who can best support you on the privacy journey, focusing on the Red (Priority 1) systems from your initial assessment.

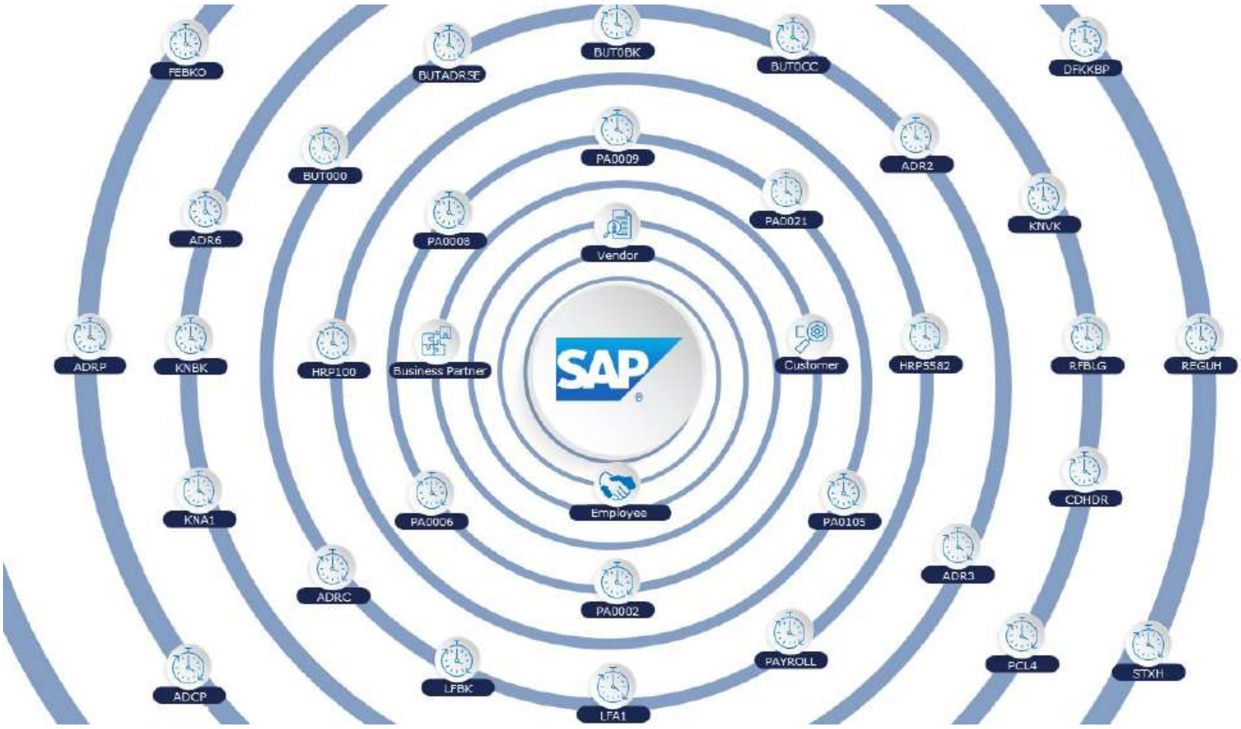
2) Find and map your PII

This is a critical first step to compliance, especially for markets where the privacy laws are new. Finding and mapping your Personally Identifiable Information (PII) allows you to demonstrate to your auditors/compliancy bodies that you have a clear understanding of the PII risk in your environment, and a plan to resolution. We have noticed at many clients in Europe that in cases where the client could prove they had started the process, the governing body would give the time to resolve the issue; whereas companies ignoring the issue completely have been more likely to be fined.

For an SAP system, the standard delivered data model is fairly complex. For example, a common business scenario could be as follows:

- You have an Employee in your environment, where you will capture the name, contact details, pay information, ID numbers, next of kin data and more, all populated into the employee 'Infotype' tables.
- That Employee works on a project for your business. During this time, the Employee travels and incurs some expenses against the project. So, their data is replicated into the Vendor tables in SAP.
- Due to the finance set-up or version of SAP you are running, the same details are also replicated to a Business Partner Object.
- This same Employee purchases something from your business and therefore becomes a Customer. Again, the personal details of name, address, telephone, bank details will be stored into another set of tables.
- The resulting interrelated web of tables and fields containing PII easily stretches into thousands of technical locations.
- The privacy law considers the Data Subject as a single being, not that they exist as an Employee or a Vendor or a Customer. If you have a Right to Deletion request, you have to be certain of the whole Data Subject's relevance for retention to make your decision.

This scenario explains one of the cases in which AI and Machine Learning cannot effectively manage SAP data for privacy; you need specific domain knowledge built into your software to achieve complete and consistent data removal.



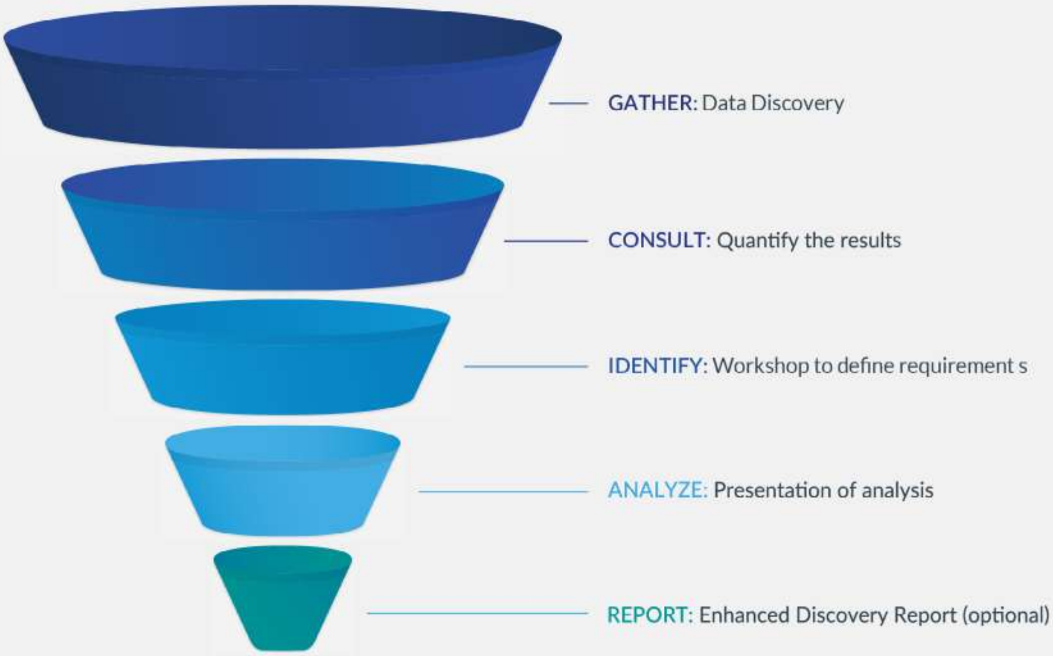
What about customisations in SAP?

Most companies will have customised their SAP instance over the years to have specific processes that function the way they need them to for their industry and business. In SAP, these are called Z or Y tables. You can also purchase add-ons which provide their own tables and fields which may contain PII (these will always start with a / in other words: /addon/table).

So how can you map and understand all of this?

As SAP data management specialists, EPI-USE Labs has already mapped the standard SAP tables and Object integrations, both within one SAP system, and also between multiple SAP systems. Having completed consistent data copies for over two decades, we have the domain knowledge of the SAP solution to be able to accurately simplify and accelerate your mapping process.

We have designed an SAP-specific data privacy assessment service, where we use the domain knowledge along with software written for this purpose to analyse the dictionary of tables and fields in your environment and highlight the fields which possibly contain PII. Manual analysis of the results is completed, and workshops held with the same key stakeholders from the Impact and Risk Assessment to define the approach to compliance in both Production and non-production per type of PII.


GATHER: Data Discovery
CONSULT: Quantify the results
IDENTIFY: Workshop to define requirement s
ANALYZE: Presentation of analysis
REPORT: Enhanced Discovery Report (optional)

More information on this service is available on our website.

The output of this project phase would be a technical and functional specification of the PII risk and locations in your specific SAP instance. It includes both the business requirement of how data will be handled in the different SAP environments, and the technical PII map of sensitive data types. I recommend this document is also shared with your audit teams. Following sign-off, you can move forward to the next phase of analysis.

3) Review access risk and controls

Now that you know where the PII is in your SAP system, the first control that can be put in place is user authorisation and access control, restricting who can access PII, and ensuring that access is justified. Many businesses already have some GRC (Governance, Risk management and Compliance) processes; however historically these will have been aimed at Segregation of Duties (SoD) and potential fraud. These new data privacy laws require PII access risks to be added to the mix.

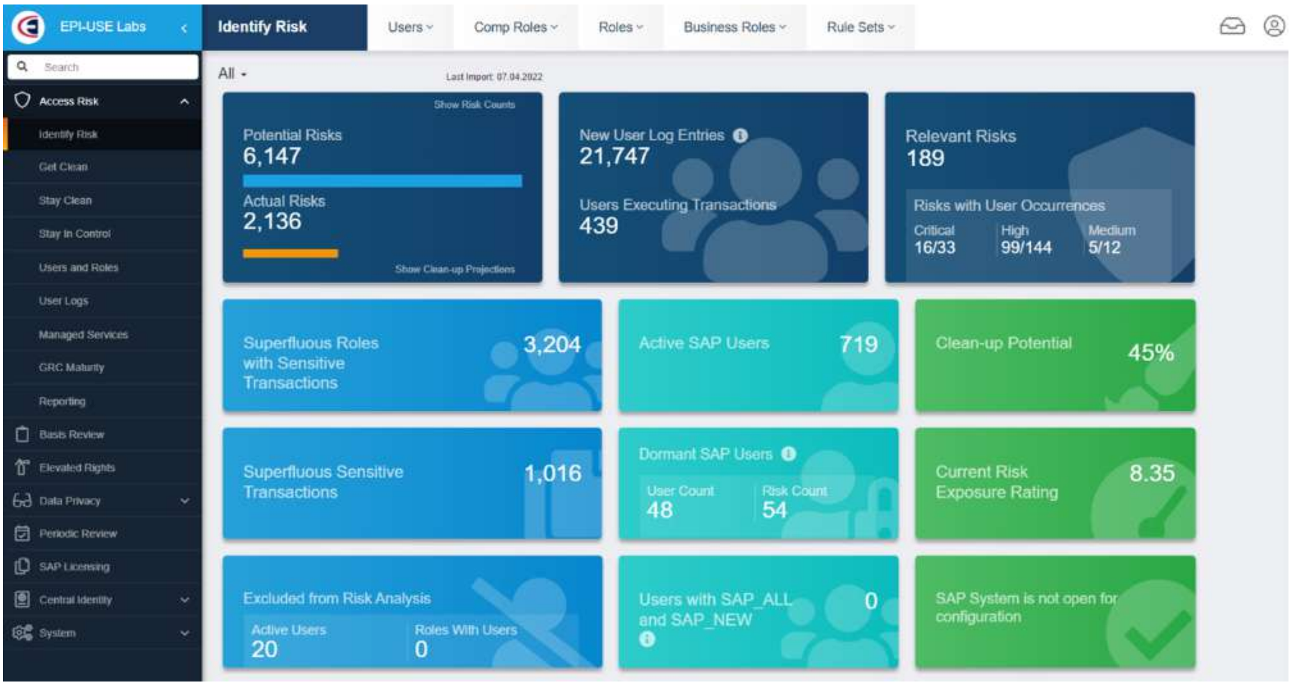
You now need to consider who can access the different types of PII; for example, ensuring that non-HR staff can't access HR details; and that HR staff can't access financial information. In addition, you need to consider access to the same functional data being available from different geographical locations, and the impacts of the local privacy laws on that access.

In the new world of cloud applications linked to larger SAP instances, you also have to be able to map and view authorisations from between multiple systems.

Partnership with Soterion: solving GRC for SAP

EPI-USE Labs formed a close partnership with Soterion whose compliance software solves GRC for SAP® clients. Traditional SAP GRC appliances are not built to be adjusted easily; but Soterion can provide accelerators on a fully customisable platform. Our partnership brings together powerful complementary solutions, knowledge and experience, to help our clients address compliance with global data privacy legislation.

Similar to PII mapping, the starting point needs to be mapping who can access what. Soterion's solutions allow you to get a first look, with a download of authorisation data and logs which will be uploaded to your own instance of Soterion.
The accelerator rulesets which are pre-configured in the software are executed, providing an initial view of risks.



Last Import: 07.04.2022

Potential Risks
6,147

Actual Risks
2,136

New User Log Entries
21,747

Users Executing Transactions
439

Relevant Risks
189

Risks with User Occurrences

Critical	High	Medium
16/33	99/144	5/12

Superfluous Roles with Sensitive Transactions 3,204

Active SAP Users 719

Clean-up Potential 45%

Superfluous Sensitive Transactions 1,016

Dormant SAP Users

User Count	Risk Count
48	54

Current Risk Exposure Rating 8.35

Excluded from Risk Analysis

Active Users	Roles With Users
20	0

Users with SAP_ALL and SAP_NEW 0

SAP System is not open for configuration

Soterion reports show the difference between Potential risks and Actual risks; the difference being users who have authorisation that may pose a risk, and users who are actively using these authorisations. They can chart a RAG (Red, Amber, Green) status of your current risk and possible risk reduction from controls being implemented.

Soterion provide delivered rulesets to cater for:

Privacy data access risks

Most GRC solutions are focused on segregation of duties and fraud avoidance. Soterion peforms these functions, and also has built a ruleset to analyze who has access to PII data.

Segregation of Duties (SoD)

Who has access to both submit and approve payments, for example? Soterion will identify all the users who hold conflicting access in the system.

Cross-legal jurisdiction data access

Can your users from the US access European employee and customer data, or vice versa? If yes, which users would be effected in creating a Data Shield?

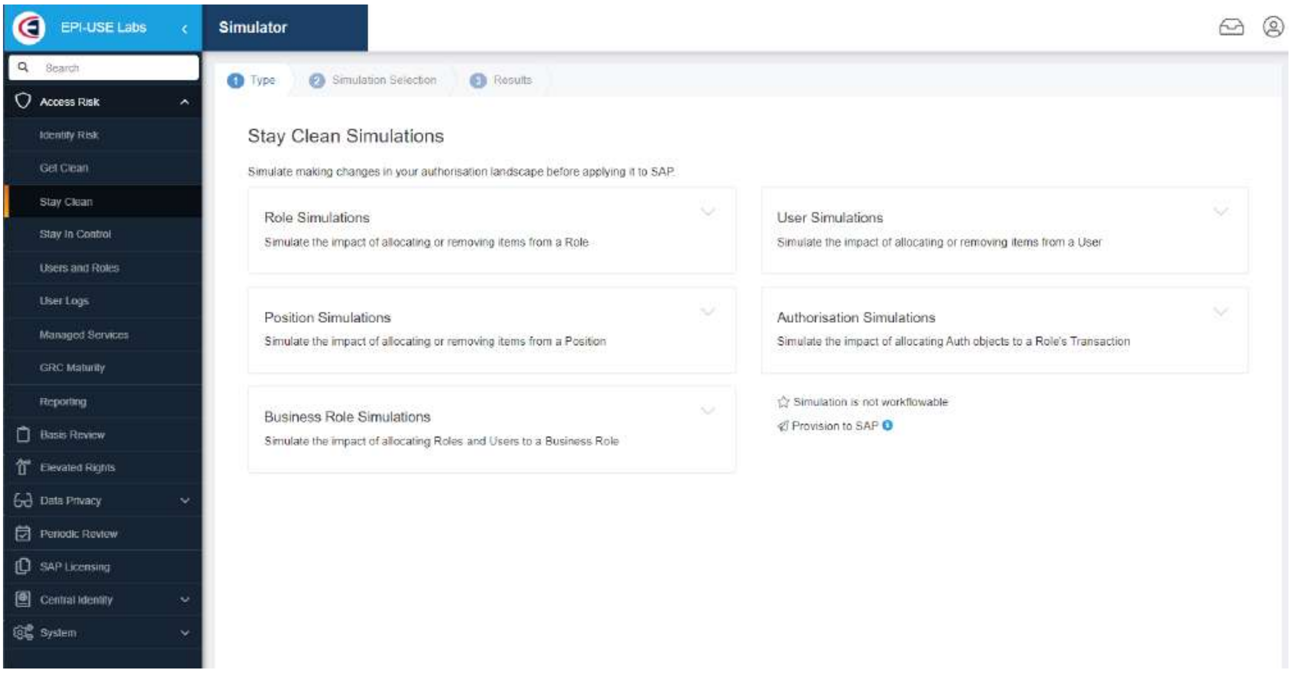
Critical transaction risk

Who has direct access for table maintenance, or can run programs directly? Is Vendor and Customer maintenance restricted to the correct people?

Once the initial assessment is complete, you need to start the process of cleaning up these risks. With the differentiation of Potential versus Actual risks, you have a clear starting point to reduce your Potential risks. These users have authorisations that they never use, so you can look at removing superfluous roles.

Actual risks require a more detailed analysis. To effectively redesign these authorisations, engaging with the business is essential. I recommend an iterative project, prioritising groups of users in similar functional areas with the same identified risks; then reviewing the role structures and allocations, and redesigning the authorisation model to remove the risks. Soterion can help with Role Simulations, confirming the impact on risks of the changes you make before you make them.

Through this controlled roll-out, you can provide sufficient change control points and a clear compliance plan for access risk management.



Stay Clean Simulations

Simulate making changes in your authorisation landscape before applying it to SAP.

Role Simulations
Simulate the impact of allocating or removing items from a Role

User Simulations
Simulate the impact of allocating or removing items from a User

Position Simulations
Simulate the impact of allocating or removing items from a Position

Authorisation Simulations
Simulate the impact of allocating Auth objects to a Role's Transaction

Business Role Simulations
Simulate the impact of allocating Roles and Users to a Business Role

☆ Simulation is not workflowable
Provision to SAP

EPI-USE Labs' clients who have used Soterion solutions complete the implementation of the software within a week to identify the risk. They then model their longer-running role redesign project according to their needs. With a plan in place to tackle risks, and active management in place, you can achieve control and improve your compliancy standing after the one-week implementation.

4) Clean up the backlog in Production

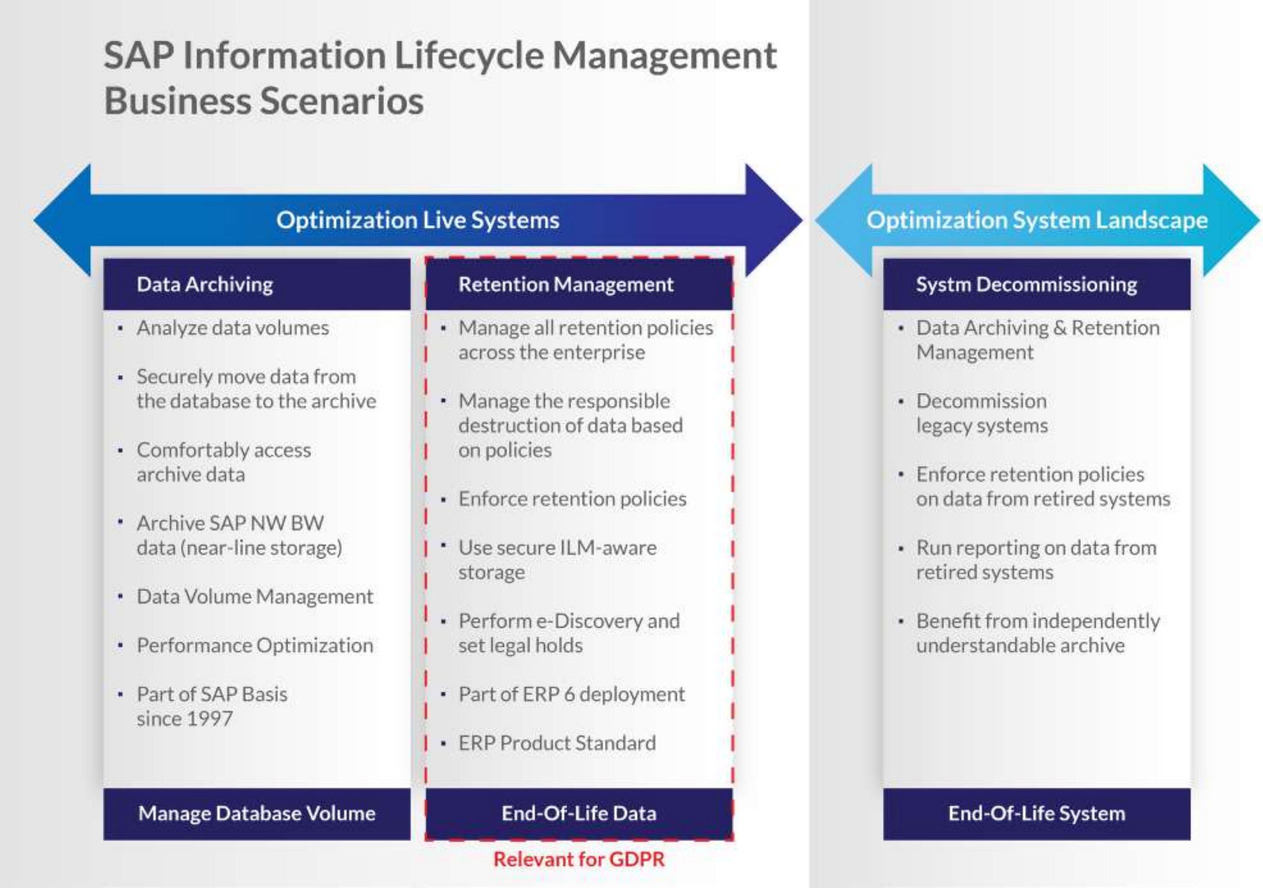
Clients who have been running SAP for multiple years have been actively collecting data for all that time, and storing it. In most cases, you will find that all that Production data has been copied into multiple copies for development, testing or training purposes.

When GDPR first launched in Europe, our approach was to suggest that you would tackle the Production copies first, thus reducing the target. This is still an option; but after working with our clients, we realised that the first priority should be getting Production under control. That way, the next time a copy is taken, it will already be more compliant throughout the landscape.

I recommend running a System and Landscape Optimisation (SLO) project. There are two main approaches to these clean-ups:

- SAP Infrastructure Lifecycle Manager (ILM): Provided by SAP, this will create a deletion job for the whole record and all related data.
- Data Redaction (from EPI-USE Labs): Our proprietary software is built to selectively remove just the PII from a record, leaving the referential integrity of the record intact, including your business financial records.

SAP ILM (7.02) was released in 2011, intended as an archiving tooling for SAP data. Once GDPR went live in 2018, it was announced as the GDPR solution too.



SAP Information Lifecycle Management Business Scenarios

Optimization Live Systems

Optimization System Landscape

Data Archiving

- Analyze data volumes
- Securely move data from the database to the archive
- Comfortably access archive data
- Archive SAP NW BW data (near-line storage)
- Data Volume Management
- Performance Optimization
- Part of SAP Basis since 1997

Manage Database Volume

Retention Management

- Manage all retention policies across the enterprise
- Manage the responsible destruction of data based on policies
- Enforce retention policies
- Use secure ILM-aware storage
- Perform e-Discovery and set legal holds
- Part of ERP 6 deployment
- ERP Product Standard

End-Of-Life Data

Relevant for GDPR

Systm Decommissioning

- Data Archiving & Retention Management
- Decommission legacy systems
- Enforce retention policies on data from retired systems
- Run reporting on data from retired systems
- Benefit from independently understandable archive

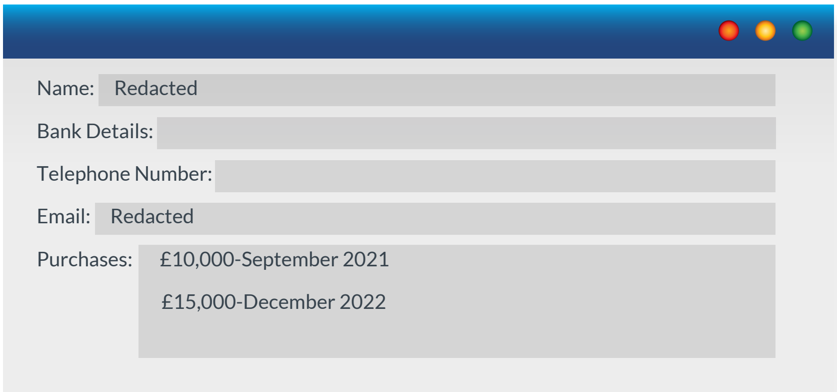
End-Of-Life System

Courtesy of SAP

Remove or redact data?

Because of the referential integrity of the SAP solution, it is not possible to simply remove just a Customer or Vendor from a finance system. Using ILM, you must remove the Customer and all associated sales/finance data, otherwise you create a system consistency issue.

Believing that you would then lose valuable business data to avoid errors, we designed the Redaction functionality, where the Customer record remains with all its associated transactions, but the sensitive PII data has been removed or replaced with a clearly demarked value. The resulting record would be similar to this:



Name:	Redacted
Bank Details:	
Telephone Number:	
Email:	Redacted
Purchases:	£10,000-September 2021 £15,000-December 2022

With the Redaction approach, you can also have different retention periods for different timelines, rather than a full deletion.

To achieve the Production clean-up, there are two policies to review:

- Data Retention Policy – defining which data should be removed after which time periods. This can be individual data per table, or a list for core Data Subjects – i.e., Employees, Customers or Vendors.
- Data Redaction Policy – defining per table field what action should be taken when the retention period is triggered.

For the initial clean-up, I recommend that the business takes responsibility for defining the list of Data Subjects to be removed. We would provide a technical retention report to define the initial input list based on the business requirements. The client is then responsible for validation and business sign-off of the list for removal.

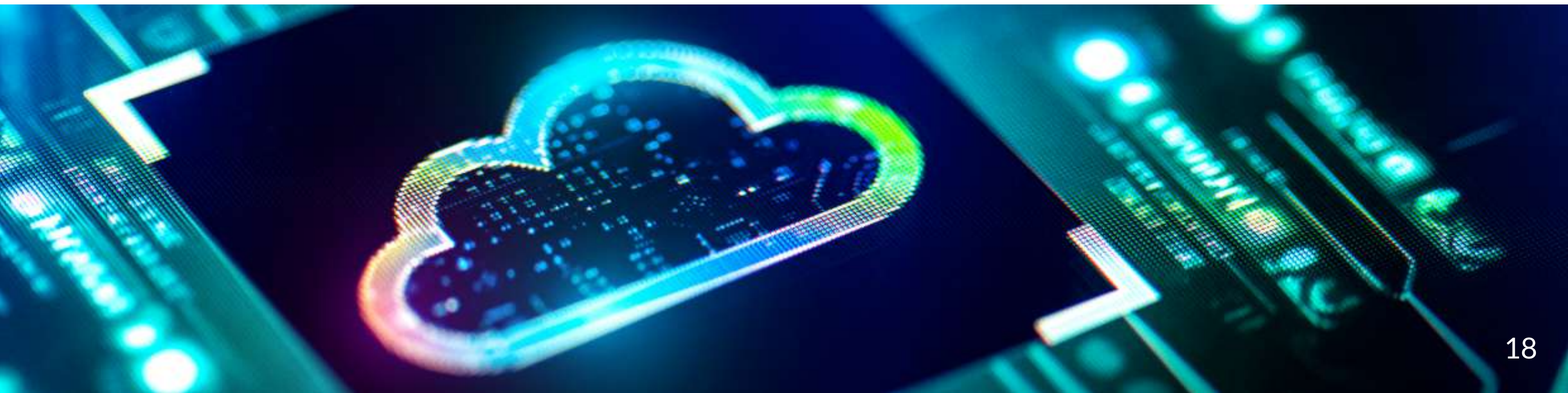
EPI-USE Labs provides the Data Transform platform with pre-delivered accelerator policies for the standard SAP data in scope, which can be fully extended to customised needs.

Typically, I recommend at least three test cycles:

- Unit testing – to be completed by EPI-USE Labs to confirm requirement to output confirmation.
- Acceptance testing – both positive and negative testing; confirmation that the request data has been removed, but also that more data than is needed hasn't been removed.
- Integration and regression testing – Confirmation that the removed data has not impacted any inter-system connectivity or processes adversely.

The second and third test cycles would be the responsibility of the business.

This first clean-up is recommended to be run as a full Production cut-over, with back-up restore options, clear process controls and tracking in place. Having run many such cutovers in my career, I can't emphasise strongly enough the advantages of a full-dress rehearsal of activities to iron out an hour-by-hour cut-over plan.



5) Manage PII in Production copies

Following changes such as

- tax year changes to Payroll,
- new processes and developments,
- system upgrades, or
- re-platforming,

a business needs to make sure their processes still function without impacting the effective running of the business.

To do this, full copies of the Production databases will often be taken throughout a year, and all data replicated into Development, Quality and pre-Production systems. Many clients will also have a training instance or separate long-term project track of SAP instances. This means the Production data has been proliferated into multiple additional systems with different use-cases for the data captured.

Informed and explicit consent of testing data?

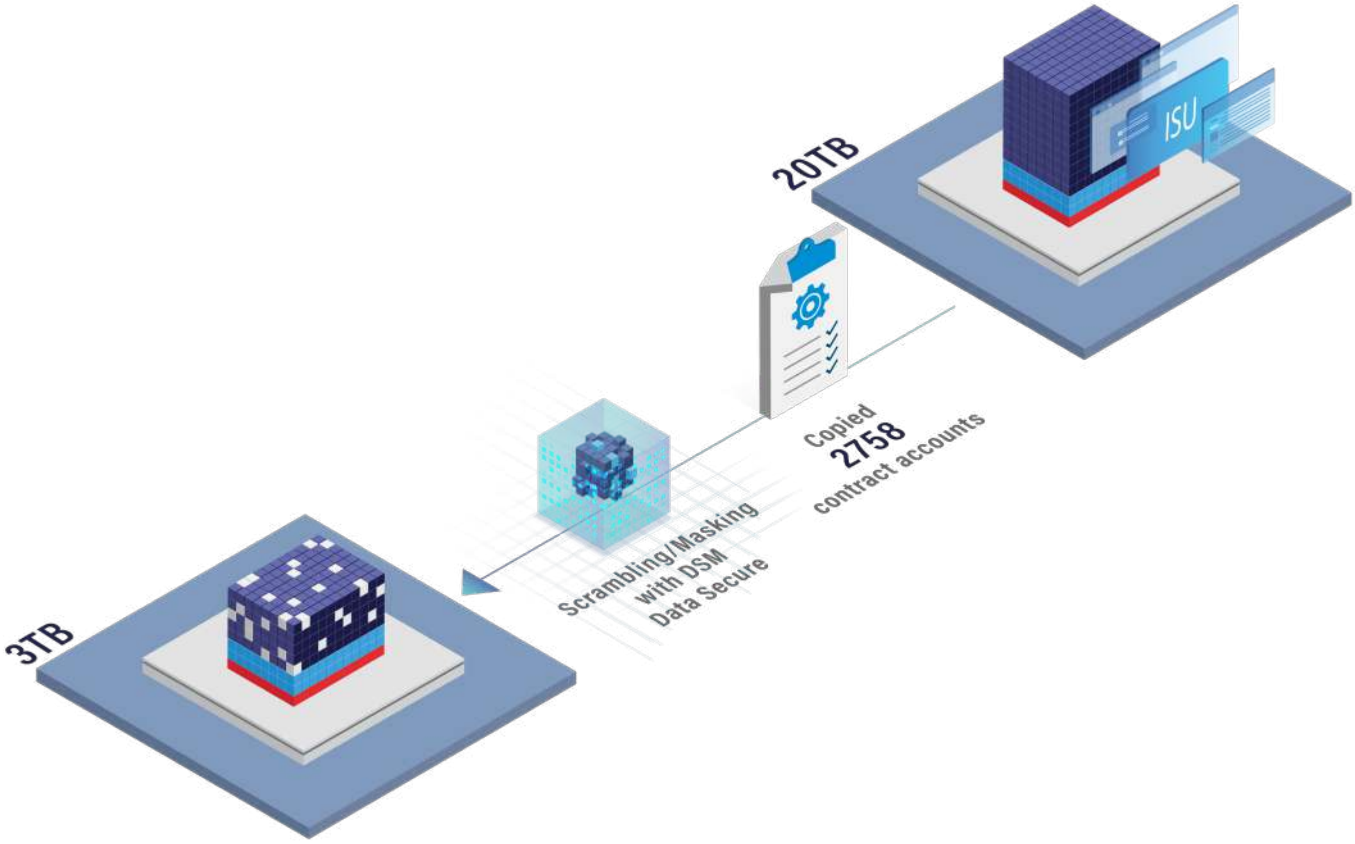
Most of the data privacy laws refer to the need for informed and explicit consent for the use case of the data you capture as a business. Most companies have not gathered this consent for using the data for testing. Even if you did decide to go down this route, and contact all Employees, Customers and Suppliers to gather terms for consent, there is still the problem of non-consent. For instance, if you have 10,000 Customers, and 100 refuse consent, if your only option is to copy the full database, you now can no longer take copies from Production.

Some software vendors on the market offer solutions which provide masking (sometimes referred to as User Interface (UI) Masking). This is where the data remains unchanged in the database, but an interception is completed when users try to access the data through the UI and either cypher or restrict visibility of PII. The issue with UI masking is that any access to the database directly doesn't go through the UI, as such no interception can occur. Usually, external data breaches and ransomware attacks would not use the UI, but make use of direct server access once network protections are breached. For this reason, personally I do not believe that UI masking complies with the data privacy laws.

A secure alternative

EPI-USE Labs' Data Secure, part of the Data Sync Manager (DSM) Suite, is an alternative to both UI masking and Consent Management. For over a decade, Data Secure has been directly modifying the values of PII fields in the database itself. The framework designed avoids the use of cyphers and seed tables which can be reversed, and instead focuses on pattern-breaking where each field is calculated independently and then aligned through our specialist domain mapping. The solution is also designed to replace names with names, and bank details as valid formatted random bank details.

The aim is to ensure that your SAP data still has valid values which will pass system validations, but without leaving the actual PII information associated to the record. With accelerator policies provided for the standard SAP model, and a fully customisable framework, you can target the PII in non-production for consistent replacement, thus removing the PII risk. Read more about Data Secure.

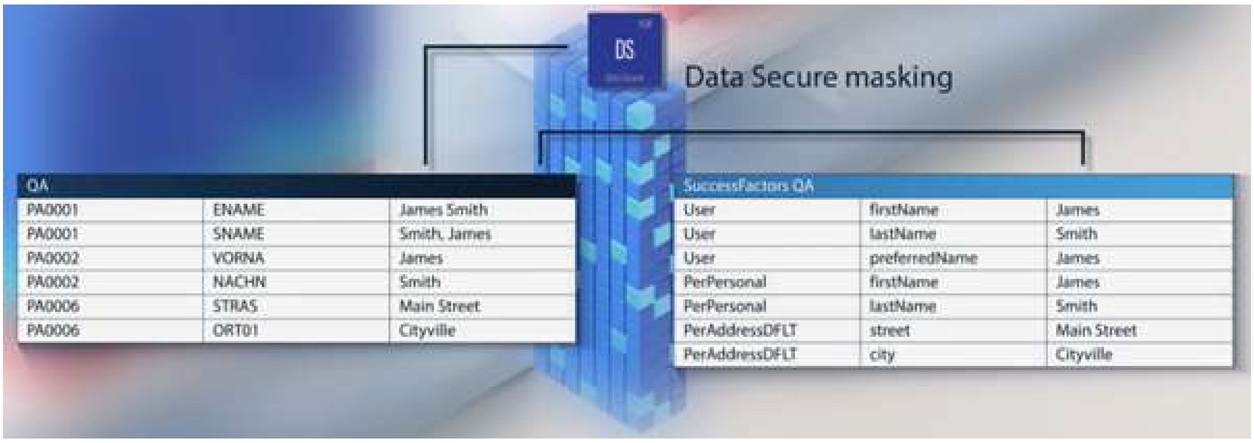


Multiple system types

Many clients we work with have multiple system types to contend with, such as connected cloud applications (CONCUR, ARIBA or SUCCESSFACTORS).

I have two recommendations:

- Firstly, where it is an OData-connected cloud application, we have designed a cloud integration platform that allows the data to be replicated from the cloud application into the scrambling provided by Data Secure, providing cross-sys tem integrated scrambling.
  In this example, an SAP Employee and SuccessFactors Entity data are being anonymised to the same new values.



QA		
PA0001	ENAME	James Smith
PA0001	SNAME	Smith, James
PA0002	VORNA	James
PA0002	NACHN	Smith
PA0006	STRAS	Main Street
PA0006	ORT01	Cityville

SuccessFactors QA		
User	firstName	James
User	lastName	Smith
User	preferredName	James
PerPersonal	firstName	James
PerPersonal	lastName	Smith
PerAddressDFLT	street	Main Street
PerAddressDFLT	city	Cityville

- However, there are multiple different types of systems and API connections. Although the Data Secure solution has other APIs available, we have also reviewed the other industry participants and identified a key partner to support non-SAP appliances. So, the second recommendation is to review DatProf for your non-SAP appliances. Capable of taking an input list of keys and new values, DatProf can take an extract of the SAP scrambling completed by Data Secure and use this to match the new scrambled data in all connected appliances.

6) Handle Data Subject Access Requests (DSARs)

Many previous data privacy laws made provision for the principle of Subject Access Requests; in other words, that any individual person can request the information that a company holds about them. The main change in the more recent legislation is that the time period to respond is far stricter.

As these requirements have existed for some time, many businesses already have processes in place for responding to a Right to Access request; however, these are often manual and time-consuming processes.

With the media attention that the data privacy laws, their enforcements and court cases are getting, the volume of Access Requests has been increasing. I am also aware of social media groups who will pick targets, and all contact a company at the same time.

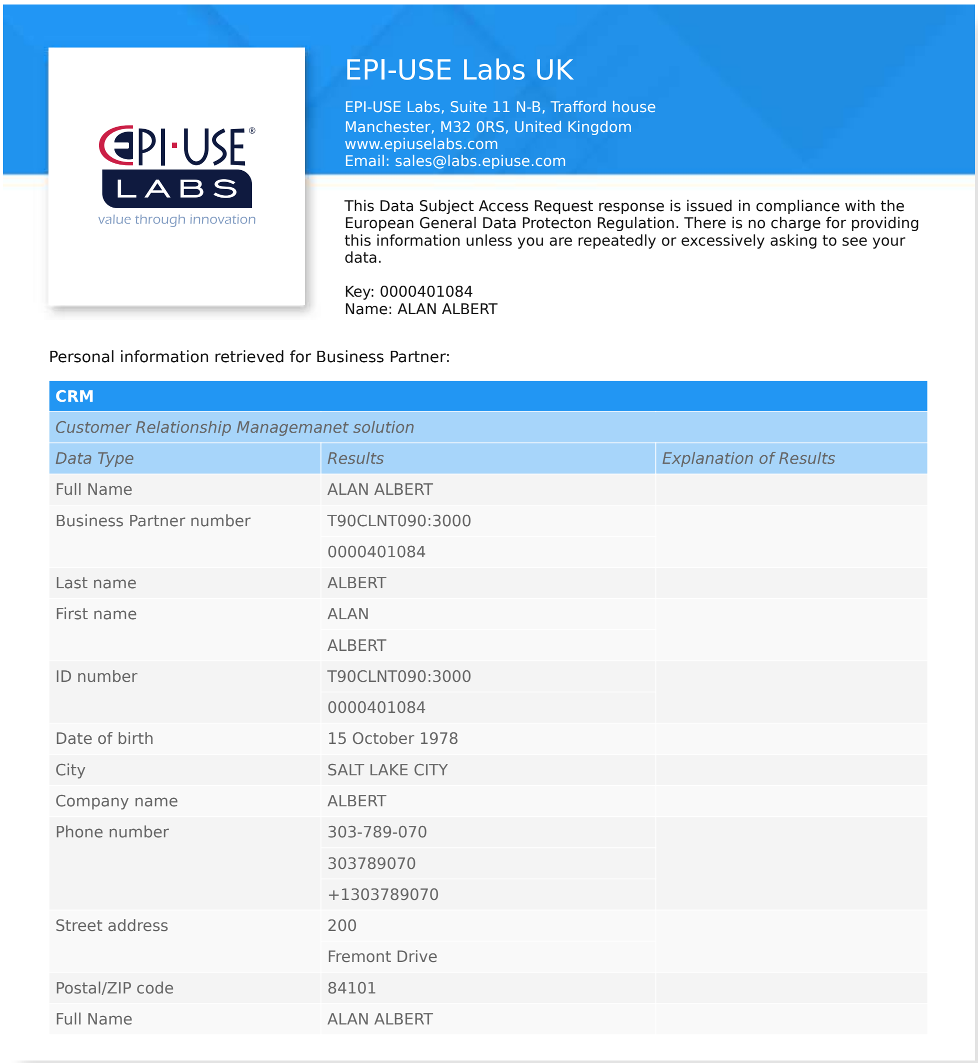
A more automated and efficient response to an access request is needed to manage these spikes in requests through your normal customer-facing teams. Our experience in Europe has been that if you are able to respond quickly with a formatted detailed document to your customer, they are far less likely to follow up with additional requests.

Responding quickly to DSARs

EPI-USE Labs' Data Disclose uses the same mapping used in the data removal and scrambling solutions; we already know where all the PII on an individual is stored. It is able to search multiple SAP systems and connected cloud applications in a single output report, collating the information into a branded formatted PDF.

The PDF file is mandatorily saved with encryption, and password protected; so, the file can be shared via email to the Data Subject making the request. It could also be printed and posted, depending on your business process.
Finding a real-time front-office solution to respond to the Right to Access will streamline compliance with the privacy laws. We have found that the focus and volume of requests is generally higher for individual customer-facing businesses, such as in retail, healthcare and utilities. In these industries, a solution like Data Disclose is essential.

Read more about Data Disclose



EPI-USE Labs UK

EPI-USE Labs, Suite 11 N-B, Trafford house
Manchester, M32 0RS, United Kingdom
www.epiuselabs.com
Email: sales@labs.epiuse.com

This Data Subject Access Request response is issued in compliance with the European General Data Protecton Regulation. There is no charge for providing this information unless you are repeatedly or excessively asking to see your data.

Key: 0000401084
Name: ALAN ALBERT

Personal information retrieved for Business Partner:

CRM

Customer Relationship Managemanet solution

Data Type	*Results*	*Explanation of Results*
Full Name	ALAN ALBERT	
Business Partner number	T90CLNT090:3000	
	0000401084	
Last name	ALBERT	
First name	ALAN	
	ALBERT	
ID number	T90CLNT090:3000	
	0000401084	
Date of birth	15 October 1978	
City	SALT LAKE CITY	
Company name	ALBERT	
Phone number	303-789-070	
	303789070	
	+1303789070	
Street address	200	
	Fremont Drive	
Postal/ZIP code	84101	
Full Name	ALAN ALBERT	

7) Process individual Right to Deletion requests

As well as the Right to Access, Data Subjects are now granted the Right to Deletion. If your company has no live legal justification to retain the data, it must be removed.

When working with our clients, I always find it interesting that the differing responsibilities between business and IT teams is often quite challenging in defining these processes. In most scenarios, the business is the data owner; data quality and management within the Production system is their responsibility, but the system processes which create, modify or remove data are provided by the IT teams. As such, the privacy compliance process is a business problem that requires an IT solution to complete. I have been in many meetings where the business team has asked IT to run the removal system, but IT will refuse, as they don't own the data they are being asked to process.

Of course, the answer is that it must be a conjoined effort. That is why the solutions developed at EPI-USE Labs have been designed with front office business users in mind, so the business can be self-sufficient on individual requests; however, we also have automated large-scale retention processing available for the IT team to run as a standard batch job. This way, IT never has to take responsibility for the data, and the business team is not responsible to batch system processes – hopefully keeping everyone happy.

As discussed earlier in this document, I strongly recommend the redaction of sensitive data, rather than complete deletion or UI masking. The definition of redaction is that the sensitive data can be removed or forced to a constant value – in other words 'redacted' in the database. This means that any access through transactions, programmes or external APIs will only return anonymised information.

However, we do not change the key values, relationships between data items in the SAP database or business intelligence, which you can maintain in your system. In short, an Employee record will still exist; you will still know the gender, race or sexual orientation; but you don't know the name, address, telephone number or email address for the employee. Through this process, business intelligence is maintained, but PII is removed, thus adhering with the privacy laws.

Data Disclose and Data Redact

Using EPI-USE Labs' Data Disclose, you can search to find the relevant SAP keys related to the Data Subject's information. For example, searching on the Name, Telephone number and Postal/zip code, will probably return a single Data Subject's Employee, Customer or Supplier record. Following identification, you can submit the individual to the Redaction Workflow. The software is designed to maintain a segregation of duty and authorisation control so the same person could not submit and approve a data removal.

The Redaction Workflow will create a case in EPI-USE Labs' Data Redact solution. Data Redact has multiple controls in place to ensure that only valid keys can be submitted; the executed removal process can only be approved by dedicated administrators, and no changes can be made by users. These controls are paramount for any Production removal programme. However, you also need a process which can be managed on a daily basis by your Production users; this edict of useability is the highest priority to me for any of these individual rights.

Once an authorised user for Data Redact opens the work queue, they are able to see the Redaction Requests for objects they are authorised to process. From here, they can view the Data Subject's data, and confirm if this Request for Deletion will be accepted or rejected. If accepted, then a change-controlled policy of all mapped PII fields will be executed, either clearing the value or setting a constant replacement value as such de-sensitising the record in your system.

A multi-policy requirement

Most business will have more than one Data Redaction policy for different data items and different time periods. The example of an employee below demonstrates a common scenario:

Policy 1: 6 months after leaving employment	Policy 2: 4 years after leaving employment	Policy 3: 7-20 years after leaving employment
Commonly removed fields: Next of kin information Bank details Appraisal / notes data	Commonly removed fields: Telephone numbers Email Addresses Company car registration Passport / Drivers licence	Commonly removed fields: Name Address Tax details All other data

These multi-policy requirements are common, and I recommend this approach be considered for all data removal requirements.

Read more about Data Redact

8) Proactive identification of Data Subjects

In addition to the individual Requests for Deletion, companies are now required to manage proactive identification of Data Subjects that should be removed from their systems. These are typically referred to as data retention requirements.

Data Retention questions

Common questions I get from many of our clients include:

What laws govern my international employees?

Essentially, this boils down to where your Data Subjects are from, not where they live now.
In many cases, the regulations cover the Data Subject according to their nationality, not their current address. When thinking about your retention periods, it is important to make distinctions for the various rules which will apply for different nationalities.

Does it have to be one rule for everything?

Certainly not; in fact, I would not recommend this. Using the Employee as an example, the bank details and next of kin/family member information should be removed soon after employment is terminated; for example, after six months. However, in most countries there is a tax law requirement to maintain the national/Tax ID, Name and pay history for seven to ten years.
So, you need to consider types of data, not Data Subjects, when considering your retention requirements.

Who decides on the retention policy?

Ultimately, the Data Protection Officer is responsible for identifying the retention timelines beyond the legal justification for retaining the information.
However, to understand the functional and technical impacts of the retention criteria, the DPO will need the assistance of the business and IT teams.

We recommend a workshop process to discuss and agree these principles between all stakeholders and baseline an initial requirement. It is likely to change through delivery and testing, but a clear feasible baseline will improve the efficiency of your project.

EPI-USE Labs' Data Retain software automates the identification of an SAP Data Subject that no longer meets the retention requirement and adds them to the Data Redact queue for processing by an approved user.

Principles of the retention process

Selectors:

Identifying the initial list of Data Subjects, for example the list of Customers who were created more than X years ago, or Employees who left employment more than Y years ago.

Validators:

Individual checks to confirm if the identified Data Subjects should be processed for redaction. These Validators will be designed to remove the largest numbers first before getting to low-level transactional checks. For example, if you have checks based on the customer type and whether they have transacted within six years, you would prioritise the type check first to only check transactions on the lowest number of records.

Processors:

Selecting the appropriate policy for the data to be Redacted and creating a batch case within the Redaction Workflow.

Technical implementation timelines of the retention report are directly proportional to the requirement complexity and the volume of Data Subjects in your environment. But a key item is also the quality of the requirement to be thought-through and signed off by your business teams prior to build and test. I have been involved in projects in which this has not been the case, and a one-to-two-week job has extended into a one-to-two-month process of test and rebuild. In short, Blueprinting is essential to retention design.

9) Ongoing audit and review

It is important that data privacy compliance is not seen as a once-off project. Through normal business change, you will introduce new risks which require controls.

From a technical system point of view, this is most generally seen in the purchase of new applications or add-ons to your SAP instance. It could also be as a result of the customisation of processes, adding new custom tables containing PII data.

I recommend to all my clients that they have a regular six-to-nine-month review with their trusted privacy partner for their system.

This review will require a mini cycle of the road to compliance, as follows:

- Complete a new Data Discovery to map the PII changes in your estate
- Continue to review the access authorisation (such as through our partner Soterion's software)
- Modify the retention and redaction policies to cater for deltas to the original policy
- Process any backlogs in Production for the deltas identified
- Update and ready the front office process to handle the Right to Access and the Right to Deletion.

I typically allow a two to three-week period for an SAP system every six to nine months to have these activities completed and controlled to Production by the experts. I call this 'Privacy Policy Management'. This review cycle, agreed upfront, can be tied into your audit reviews to ensure you have the support of the solution experts when you need it.

> Thanks to Data Secure, we can anonymize all sensitive SAP HCM data, such as employee-related data, in a very short time.
>
> The biggest advantage of Data Disclose is that data integrity is guaranteed; customers' sensitive data is anonymized but all orders and items sold are still accessible. All test systems stay fully functional, and test orders are still editable.
>
> Malte Podszus, Consultant FI/CO/HR, MAPA GmbH

Conclusion

I hope that this document has proved useful to you in reviewing how to structure your privacy project; and for SAP, some of the options and partners you can confidently get involved with.

Don't underestimate the importance of getting the right partners for the technology you are managing, and of your legal compliance teams in understanding the laws.

Privacy impacts are far reaching. And with the speed at which technology and data sharing/capture is moving, the laws must be amended to keep pace, so I expect they will change again within our lifetime. Building and investing in the right team to review, adapt and move on these changes as they come through is going to be pivotal to your business.

Thank you for the time in reading this ebook. Should you have any questions, please reach out to info@labs.epiuse.com and we'll get in touch.

About the author

A little background about me and what prompted me to write this ebook.

I started my journey in SAP data management as a business user of legacy systems, involved in the design and implementation of SAP for the client. Prior to the implementation, I was a front-end system user, team lead, trainer and eventually the business analyst for Billing for the SAP implementation. This experience of front and back-office client-facing roles combined with the IT implementation and data migration experience left me with a unique perspective of both the functional and business world.

I joined EPI-USE Labs in 2016 as a technical consultant implementing the SAP ALM Data Sync Manager (DSM) software suite. The backbone of the Data Sync Manager solution is an SAP Object definition library mapping both the cross-system and internal integrations between the different SAP instances. In 2017, I began the ramp-up of EPI-USE Labs' Data Privacy Suite for SAP in Europe, providing an answer to the Right to Access, Right to Deletion and proactive management of PII. Through this role I was able to define the project approach best suited to our clients, supporting the full project lifecycle, from requirements gathering to implementation and go-live. In 2022, I took up my global role supporting all regional teams of the EPI-USE Labs business.

So, in summary, I have supported more than 50 privacy projects on four continents and in thirteen countries subject to differing privacy laws.

I decided to write this ebook to describe the lessons I have learnt through these projects. I hope it has given you some insights into your data privacy journey.

James Watson
Line of Business Owner –
Privacy, Risk and Industry Solutions at EPI-USE Labs

As a global software solutions and managed services company, EPI-USE Labs helps you to maximise the performance, management and security of your SAP® and SAP SuccessFactors® systems. Our clients tell us every day how we have transformed their business operations. Contact us to find out how we can help you solve your business challenges.

epiuselabs.com | info@labs.epiuse.com
EPI-USE Labs is a member of groupelephant.com.

A MEMBER OF: groupelephant.com™ BEYOND CORPORATE PURPOSE