GDPR

READINESS FOR SAP COMPANIES

A Practical Guide

Published 2017

soterion

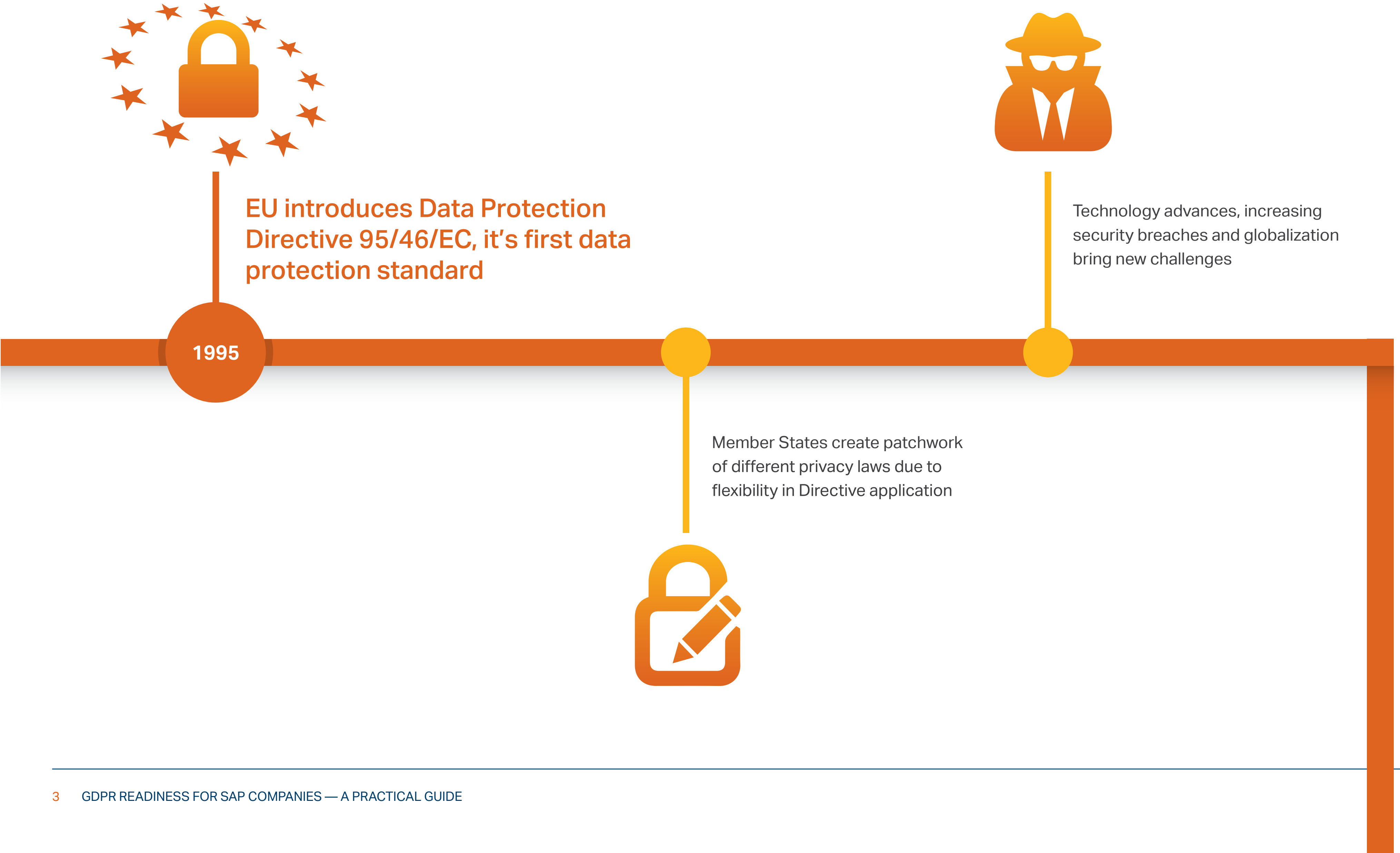
CONTENTS

GDPR **AT A GLANCE**

GDPR will take effect on 25 May 2018, establishing personal data protection as a basic human right for EU-based individuals.

The legislation's impact extends beyond EU borders to any organisation which either sells goods or services to EU data subjects, or who monitors the behaviour of EU data subjects.

GDPR sets out clear requirements to be followed by anyone processing personal data of EU-based individuals, and allows for significant fines for non-compliance of up to 4% of global annual revenue or 20 million Euros, whichever is greater.

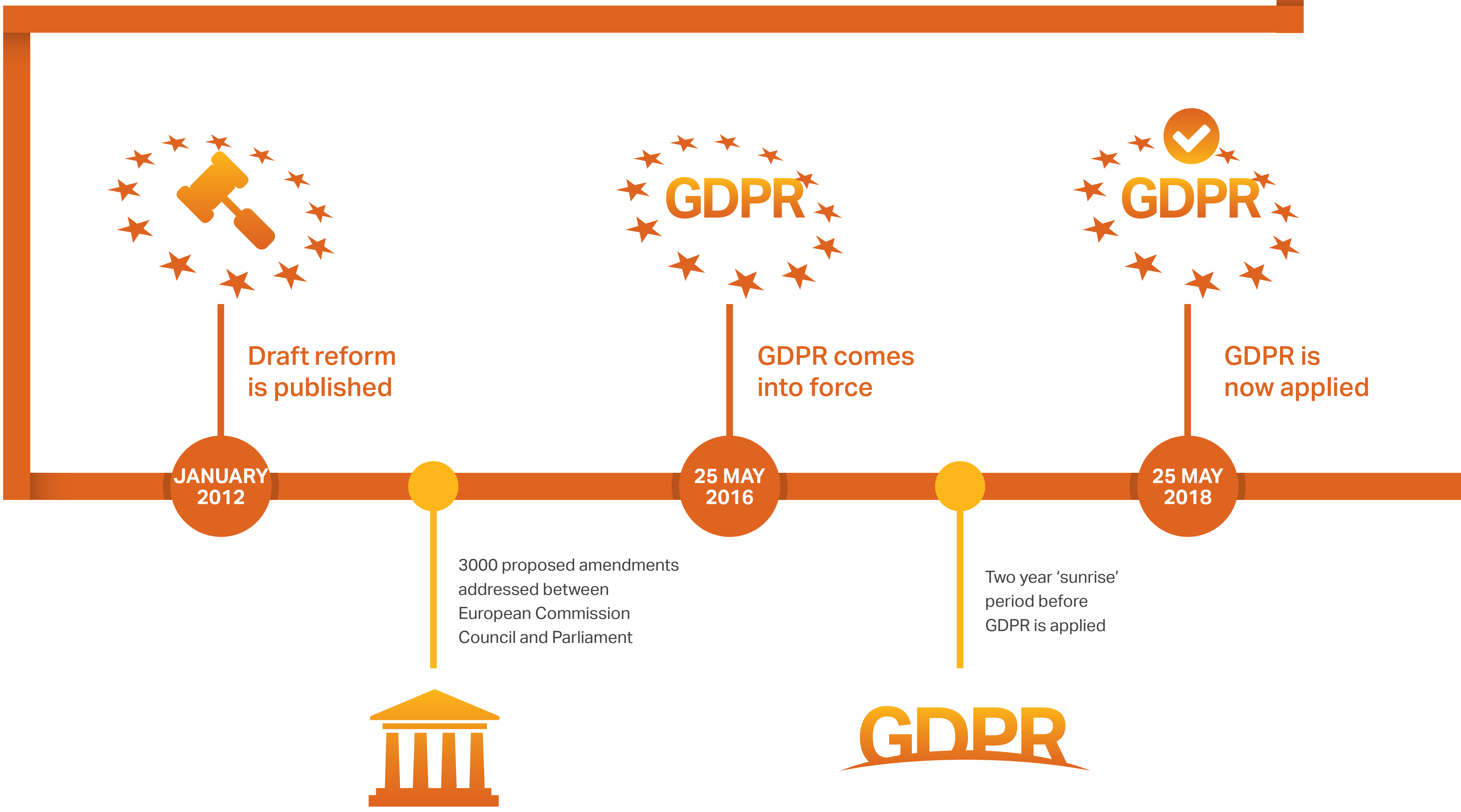


1995

EU introduces Data Protection Directive 95/46/EC, it’s first data protection standard

Member States create patchwork of different privacy laws due to flexibility in Directive application

Technology advances, increasing security breaches and globalization bring new challenges



JANUARY 2012

Draft reform is published

3000 proposed amendments addressed between European Commission Council and Parliament

25 MAY 2016

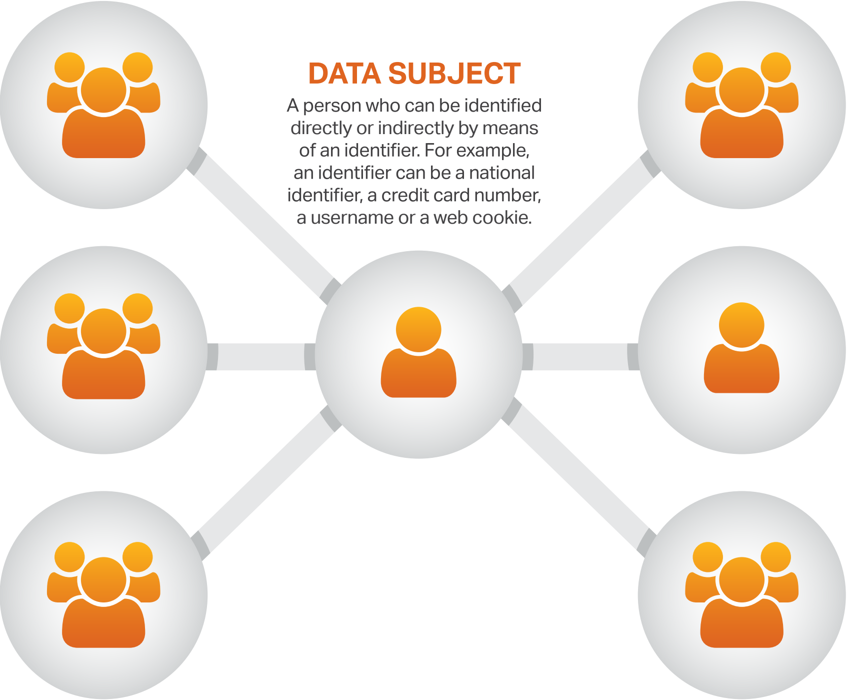
GDPR comes into force

Two year ‘sunrise’ period before GDPR is applied

25 MAY 2018

GDPR is now applied

GDPR ROLE PLAYERS



THIRD PARTY

A natural or legal person, public authority, agency or any other body other than the Data Subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, is authorized to process the data. For example, partners or subcontractors.

SUPERVISOR AUTHORITY

An independent public authority established by a Member State (known as the National Data Protection Authority under the current EU Data Protection Directive) or auditing agency.

RECIPIENT

A natural or legal person, agency or any other body to whom the personal data is disclosed. For example, an individual, a tax consultant, an insurance agent or an agency.

DATA SUBJECT

A person who can be identified directly or indirectly by means of an identifier. For example, an identifier can be a national identifier, a credit card number, a username or a web cookie.

CONTROLLER

A natural or legal person, public authority, agency or any other body who alone or jointly with others determines the purposes and means of the processing of personal data. For example, a Controller can be an organisation or CIO.

DATA PROTECTION OFFICER

An individual working for a Controller or a Processor with extensive knowledge of the data privacy laws and standards. The Data Protection Officer (DPO) shall advise the controller or the processor of their obligations according to the GDPR and shall monitor its implementation. The DPO acts as a liaison between the controller / processor and the supervisory authority. A DPO, for example, can be a Chief Security Officer (CSO) or a Security Administrator.

PROCESSOR

A natural or legal person, agency or any other body which processes Personal Data on behalf of the Controller. For example, a developer, a tester, or an analyst. A Processor can also be a cloud service provider or an outsourcing company.

EXAMPLE

A German manufacturing business, selling via its website, stores and processes personal information of EU-based individuals (Data Subjects) and therefore is required to determine the purpose and means of personal data processing (Controller). Development, testing and billing is outsourced to contractors in India (Processor), where employees copy data to their local systems for development, testing or processing. The company also partners with delivery companies (Third Parties) which use personal data to deliver goods. An independent public authority monitors the application of the GDPR (Supervisory Authority).

MAIN CHANGES

TERRITORIAL SCOPE

The regulation applies to all data Controllers and Processors storing and processing personal data of EU citizens, irrespective of where such organisations are based.

CONSENT

Consent needs to be informed, freely given, signified by a positive affirmation (Data Subject needs to do something), and capable of withdrawal at any time. Burden of proof is on the Controller.

PRIVACY IMPACT ASSESSMENTS

Before an organisation begins anything new, for example: merge with another company, automate a process, launch an initiative, a data privacy impact assessment must be completed prior to such activity.

RIGHT TO BE FORGOTTEN

The Data Subject has the right to request erasure of personal information - without undue delay - under certain circumstances.

ACCOUNTABILITY

Data Controllers and Processors must be able to demonstrate compliance, through implementation of proper policies, procedures and processes.

MANDATORY DATA PROTECTION OFFICERS

Organisations that operate in the Public Sector or are involved in large scale data monitoring or processing of sensitive data, will require suitably qualified Data Protection Officers.

BREACH NOTIFICATION

If an organisation loses or compromises data, it needs to inform the Data Authority and Date Subjects.

PENALTIES

Failure to comply with GDPR may result in penalties of up to 4% of annual global revenue or 20 million Euros, whichever is greater.

AN APPROACH
TO GDPR COMPLIANCE IN SAP ORGANISATIONS

INTRODUCTION

The introduction of General Data Protection Regulation (GDPR) has presented SAP customers with many new challenges. Confusion over the complexity and initiation of the GDPR compliance process can increase significantly when the intricacy of the SAP landscape and the immense quantity of stored data are also taken into consideration. Many companies are overwhelmed by the demands that are put on their resources when supporting multiple SAP systems (ECC, SRM, CRM etc.) and multiple SAP tiers (DEV, QAS, PRD) at the same time.

THE SAP ENVIRONMENT: PERSONAL AND SENSITIVE INFORMATION

SAP **ECC**

SAP USERS, VENDOR, CUSTOMER

Street address, Postal address, Telephone number, Tax number, Credit card number

SAP **HR**

EMPLOYEE MASTER RECORDS

Street address, Postal address, Telephone number, Tax number, Medical aid, Family dependents, Religion, Sexual orientation, Pension

SAP **BW**

SAP USERS, VENDOR, CUSTOMER, EMPLOYEES

Street address, Postal address, Telephone number, Tax number, Medical aid, Family / Dependants, Religion, Sexual orientation, Pension

SAP **CRM**

CUSTOMER

Street address, Postal address, Telephone number

SAP **SRM**

VENDOR

Street address, Postal address, Telephone number

ADDED COMPLEXITY OF A 3-TIER LANDSCAPE

PRODUCTION (PRD)	SAP **ECC**	SAP **HR**	SAP **BW**	SAP **CRM**	SAP **SRM**
QUALITY ASSURANCE (QAS)	SAP **ECC**	SAP **HR**	SAP **BW**	SAP **CRM**	SAP **SRM**
DEVELOPMENT (DEV)	SAP **ECC**	SAP **HR**	SAP **BW**	SAP **CRM**	SAP **SRM**

Whilst there are several resources available to describe the guidelines of GDPR compliance, there is a definite requirement for practical instructions on HOW to achieve compliance.

Many industry guides typically suggest the GDPR compliance process should be commenced by categorising the sensitive data handled by the organisation. This is a good starting point in principle, but in reality this is quite difficult to achieve.

For instance, a business might determine that 'ADDRESS' is a personal identifiable field, after which they will have to establish the technical name for it, as well as the large number of tables in SAP that may contain this field. In addition to assessing all the programs and transaction codes that may reference these tables, it will also have to be determined which Users have access to these sensitive data elements (tables, transaction codes, queries) based on their specific user access or permission as defined by the organisation.

> *We have developed a number of solutions with pre-defined rules which will highlight the personal and sensitive data present in an organisation's SAP environment.*

The next section will attempt to offer a practical guide on HOW we can assist an organisation to achieve GDPR compliance with respect to your SAP environments.

In order to guide organisations through the various complex phases of the GDPR process within intricate SAP environments, we have developed a basic road map which contains recommendations that are easy to understand and simple to implement. We can ensure a more holistic approach to data security by considering the SAP Production, Quality Assurance and Development environments.

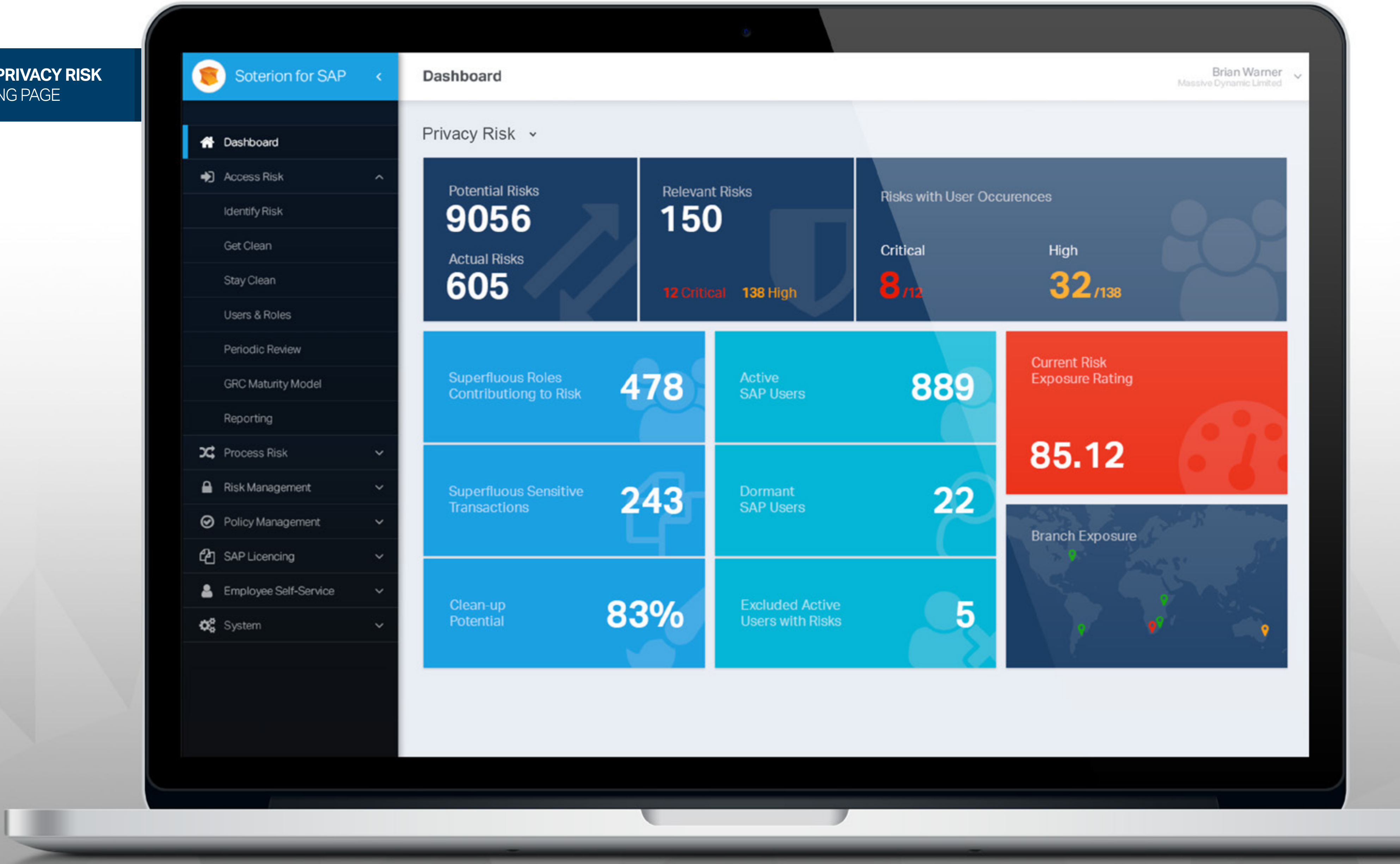
PHASES OF THE ROAD MAP

	PHASE 1: **RISK ASSESSMENT** Understand your risk exposure	PHASE 2: **RISK PREVENTION** Reduce your risk exposure	PHASE 3: **ON-GOING MONITORING** Manage your risk exposure
PRODUCTION (PRD)	GDPR **RISK IDENTIFICATION** ✓ Determine sensitive and personal data (SPD) ✓ Identify transaction or tables with SPD ✓ Identify Users and Roles who have access to SPD ARM - IDENTIFY RISK	GDPR **RISK PREVENTION** ✓ Access Risk Remediation ✓ Simulations (What-if scenarios) ✓ The right to view / to be forgotten ARM - GET CLEAN ARM - STAY CLEAN DATA DISCLOSE DATA REDACT DATA RETAIN	GDPR **MONITORING** ✓ Periodic Reviews ✓ Mitigations PERIODIC RISK MANAGER DATA RETAIN
QUALITY ASSURANCE (QAS)	GDPR **RISK IDENTIFICATION** ✓ Determine sensitive and person data (SPD) ✓ Identify transaction or tables with SPD ✓ Identify Users and Roles who have access to SPD ARM - IDENTIFY RISK	GDPR **RISK PREVENTION** ✓ Anonymization / Pseudonymisation ✓ Encryption DATA SECURE	
DEVELOPMENT (DEV)	GDPR **RISK IDENTIFICATION** ✓ Determine sensitive / person data (SPD) ✓ Identify transaction / tables with SPD ✓ Identify Users & Roles who have access to SPD ARM - IDENTIFY RISK	GDPR **RISK PREVENTION** ✓ Anonymization / Pseudonymisation ✓ Encryption DATA SECURE	

GDPR
ACCESS RISK AND DATA ASSESSMENT

soterion

USER PRIVACY RISK
LANDING PAGE



Soterion for SAP

- Dashboard
- Access Risk
  - Identify Risk
  - Get Clean
  - Stay Clean
  - Users & Roles
  - Periodic Review
  - GRC Maturity Model
  - Reporting
- Process Risk
- Risk Management
- Policy Management
- SAP Licencing
- Employee Self-Service
- System

Dashboard

Brian Warner
Massive Dynamic Limited

Privacy Risk

Potential Risks 9056
Actual Risks 605

Relevant Risks 150
12 Critical 138 High

Risks with User Occurences
Critical 8/12
High 32/138

Superfluous Roles Contributiong to Risk 478

Active SAP Users 889

Current Risk Exposure Rating 85.12

Superfluous Sensitive Transactions 243

Dormant SAP Users 22

Branch Exposure

Clean-up Potential 83%

Excluded Active Users with Risks 5

GDPR RISK ASSESSMENT

WHAT IS THIS?

The starting point on your GDPR compliance journey is to have an assessment on your SAP environment (PRD, QAS and DEV). This will provide you with an understanding of the impact that GDPR will have on your business. Due to the complexity of the SAP environment and sheer volumes of data stored in thousands of tables with hundreds of thousands of fields, finding who has access to the sensitive fields is as challenging as finding a needle in a haystack. The reality is that most companies running SAP would not know which Users have access to this sensitive data, especially since personal and sensitive data can be obtained in a multitude of ways through transaction codes, tables and queries.

HOW IS THIS DONE?

Due to the sheer volumn of data between the various SAP systems, performing a GDPR risk assessment manually will be a near impossible task. The most cost effective way is to make use of a GDPR access risk software. As with all access risk tools, the effectiveness of the tool is highly dependant on the quality of the GDPR rule set. We all know the expression 'garbage in, garbage out'.

Other important factors to keep in mind when looking for a GDPR access risk assessment tool are:

- Efficiency of the assessment process. As assessments are going to be done in a number of SAP systems, look for software where results can be obtained with minimal effort, time or cost.
- Displaying of the results. Find software that will provide the results of the assessment in a user-friendly manner. Avoid being sent the results in a spreadsheet format as this will make remediation very cumbersome.

IN PRODUCTION ENVIRONMENT (PRD)

SAP Production environments typically have the most fine-grained access of the three-tier landscape. However, as display access is often assigned more liberally, it is very important to know which Users have access to sensitive data and whether this is relevant for their job function. For example: XK03 (Display Vendors) may contain personal information such as telephone number, address, bank details, etc.

Recommended Product: **SOTERION GRC**
Relevant Module: ***Access Risk Manager (ARM)***

A GDPR risk assessment using Soterion's Access Risk Manager will highlight the Users and Roles that have access to sensitive and / or personal data. By incorporating Soterion's pre-defined GDPR rule set for sensitive and personal data, this assessment will give the company an indication of where the personal data resides, and who has access to this information to determine their risk exposure level.

Our GDPR assessment tools are minimally invasive, using certified SAP RFC extraction processes, and do not require any ABAP or changes to SAP. The entire process from extraction to displaying results typically takes less than a day. The results of the Soterion GDPR risk assessment are provided to the customer via a web application, providing drill-down, sorting and grouping capabilities that allow for easy interpretation of the findings.

IN QUALITY ASSURANCE ENVIRONMENT (QAS)

Previously access risk assessments focused on the Segregation of Duty (SOD) and Critical Transaction risk categories, which meant that it was sufficient to only assess the Production environment. GDPR has expanded the scope to now include a new risk category, access to personal and sensitive data, which also exists outside of the Production environment. Quality Assurance (QA) environments are typically a copy of the Production environment, which contain real personal and sensitive data. Users in QA often have wider access compared to the Production environment, in order to carry out functions such as testing.

This means that checking for access risk only in Production is no longer enough – QA and Development environments will now also need to be assessed. These environments potentially pose a greater GDPR risk to an organisation, as the normal control mechanisms usually do not apply to the non-production environments.

Recommended Product: **SOTERION GRC**
Relevant Module: ***Access Risk Manager (ARM)***

A GDPR risk assessment using Soterion's Access Risk Manager will highlight the Users and Roles that have access to sensitive and / or personal data. By incorporating Soterion's pre-defined GDPR rule set for sensitive and personal data, the assessment will give the company an indication of where the personal data resides, and who has got access to this information to determine their risk exposure level.

> *"...the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."* Article 35

IN DEVELOPMENT ENVIRONMENT (DEV)

Development environments are typically used for configuration and development activities. Many companies assign broad and non-restrictive access permissions to Users in the Development environment. Although test data is usually used in the Development environment, there may be cases where valid personal and sensitive data is being used . In such cases a risk assessment should be performed on this environment to ensure that the appropriate controls are adopted to facilitate that the company complies to GDPR.

Recommended Product: **SOTERION GRC**
Relevant Module: ***Access Risk Manager (ARM)***

A GDPR risk assessment using Soterion's Access Risk Manager will highlight the Users and Roles that have access to sensitive and / or personal data. By incorporating Soterion's pre-defined GDPR rule set for sensitive and personal data, this assessment will give the company an indication of where the personal data resides, and who has access to this information to determine their risk exposure level.

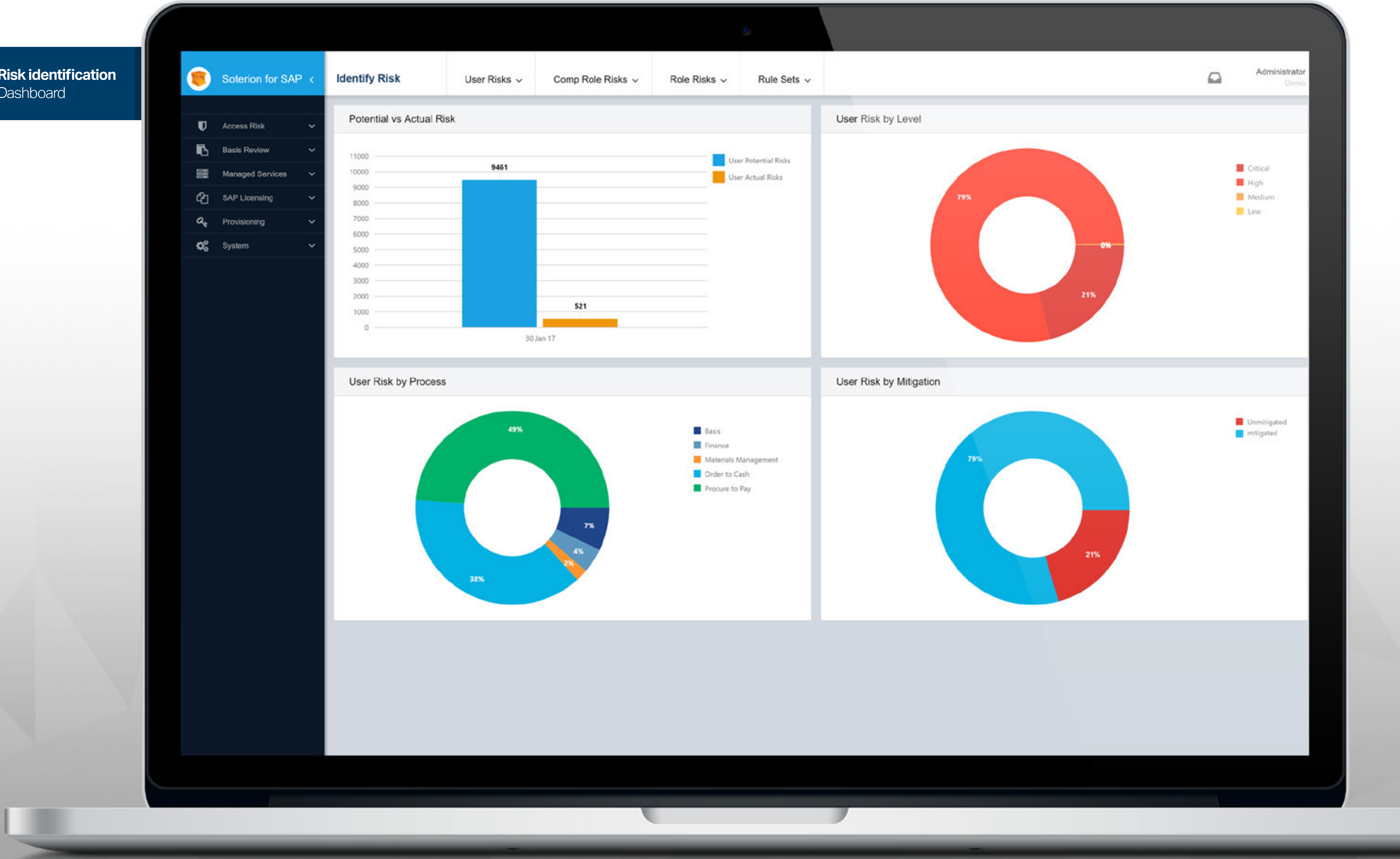
> *"...a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk..."* Recital 90

GDPR

ACCESS RISK AND DATA PREVENTION

soterion

Risk identification
Dashboard



WHAT IS THIS?

Once the GDPR risk assessment has been performed and the organisation knows their GDPR risk exposure, they should then move to the Prevention phase on the GPDR roadmap. Prevention basically equates to minimising your GDPR risk.

HOW IS THIS DONE?

There are a number of techniques that are available for the Prevention phase. Although they all have the same objective i.e. to reduce your GDPR access risk exposure, some techniques are better suited to certain SAP environments than others. At a high level, a company should attempt to remediate as much of the GDPR risk as possible. Any risk that is unavoidable should be mitigated.

The primary techniques available at this stage are:

- ✓ Access Remediation
  Removal of inappropriate access to personal and sensitive data, motivated by relevant controls defined by the business in its data governance program through policies.
- ✓ Data Scrambling
  Personal and sensitive data can be made unreadable using pseudonymization and other anonymization techniques. This is done to ensure any personal information is de-identified.
- ✓ Data Purging
  Removal of personal or sensitive data that is no longer required, or not relevant for the purpose of processing, as suggested by the GDPR.
- ✓ Mitigation
  Design and implement mitigating controls, such as using data encryption to reduce your risk exposure and ensure that only authorised individuals can decrypt and process personal information as required by the data governance program.

IN PRODUCTION ENVIRONMENT (PRD)

In Production environments access to personal and sensitive data needs to be carefully controlled, as techniques such as pseudonymisation is not appropriate on live production data. Companies should identify and remove (clean-up) the GDPR risk in their SAP PRD systems.

Recommended Product:	**SOTERION GRC**
Relevant Module:	***ARM - Get Clean***

A GDPR risk assessment using Soterion's Access Risk Manager will highlight all the Users and Roles that contain personal or sensitive data in the Production environment. By making use of the User - Transaction logs, Soterion's Get Clean functionality will highlight any unused sensitive access that can be removed without any adverse impact on the business. Clean-up Wizards provide actionable steps to remediate the access risk. In many cases this removes as much as 90% of the GDPR access risk in the Production environment.

> *"Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing."* Recital 39

> *"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed"* Article 15

Recommended Product: **SOTERION GRC**
Relevant Module: ***Allocation Simulator***

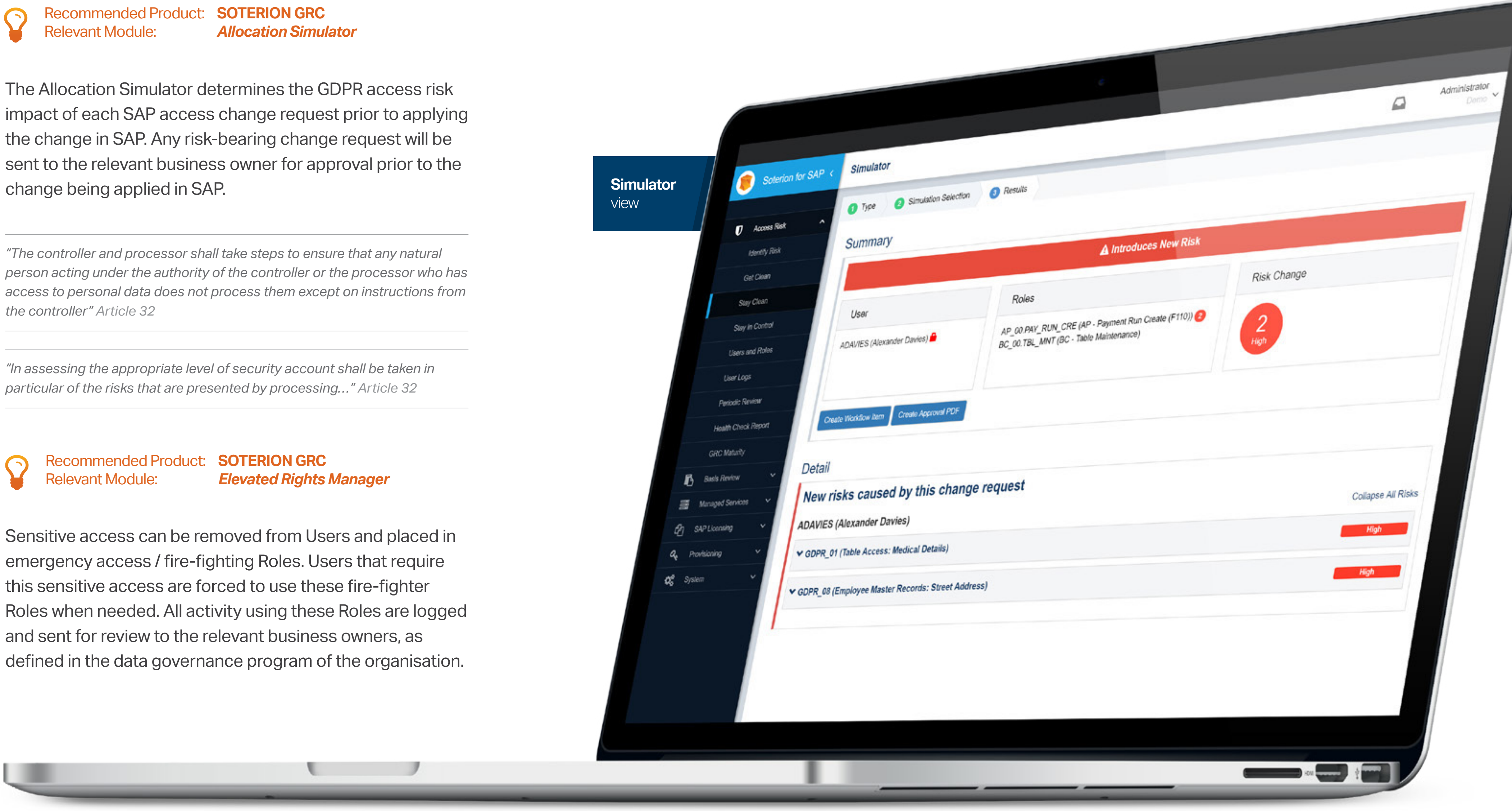
The Allocation Simulator determines the GDPR access risk impact of each SAP access change request prior to applying the change in SAP. Any risk-bearing change request will be sent to the relevant business owner for approval prior to the change being applied in SAP.

> *"The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller"* Article 32

> *"In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing…"* Article 32

Recommended Product: **SOTERION GRC**
Relevant Module: ***Elevated Rights Manager***

Sensitive access can be removed from Users and placed in emergency access / fire-fighting Roles. Users that require this sensitive access are forced to use these fire-fighter Roles when needed. All activity using these Roles are logged and sent for review to the relevant business owners, as defined in the data governance program of the organisation.



Simulator view

Simulator

Summary

⚠ Introduces New Risk

User

ADAVIES (Alexander Davies)

Roles

AP_00.PAY_RUN_CRE (AP - Payment Run Create (F110)) 2
BC_00.TBL_MNT (BC - Table Maintenance)

Risk Change

2 High

Detail

New risks caused by this change request

ADAVIES (Alexander Davies)

- GDPR_01 (Table Access: Medical Details) — High
- GDPR_08 (Employee Master Records: Street Address) — High

Recommended Product: **EPI-USE LABS DATA MANAGEMENT**
Relevant Module: ***Data Disclose***

Data Disclose is a reporting solution that can assist an organisation with the preparation of the legislation on compliance for GDPR article 15. This unique tool can instantly find, retrieve and present a subject's data footprint across the SAP landscape, as well as ERP, CRM, SRM and BW systems which are integrated with the SAP landscape's API. Data Disclose is built on a solid foundation of existing technology and intellectual property (IP) by leveraging Data Secure.

Recommended Product: **EPI-USE LABS DATA MANAGEMENT**
Relevant Module: ***Data Redact***

Data Redact can intelligently identify and alter data to ensure that an organisation complies with the relevant privacy laws by safely obfuscating enterprise data.

> *"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed"* Article 15

> *"The data subject shall have the right to obtain from the controller restriction of processing where... the controller no longer needs the personal data for the purposes of the processing"* Article 18

IN QUALITY ASSURANCE ENVIRONMENT (QAS)

Quality Assurance environments are typically a copy of SAP Production, which contain relevant personal and sensitive data. Users in QA often have more extensive access permissions compared to the production environment, in order to carry out functions such as testing. Further to this, controls are usually weak in non-production environments due to duplicated effort and cost. This makes risk remediation impractical and expensive.

Recommended Product: **EPI-USE LABS DATA MANAGEMENT**
Relevant Module: ***Data Secure***

Data Secure is a complete data-protection solution that masks SAP data to safeguard sensitive information. Most existing data-masking solutions use "in place" masking, which means that data is masked only after it has been copied to a target system.

Data Secure takes security to a completely new level with "source-side masking". This means that the data is masked before it ever leaves the source system. The original sensitive data is never duplicated so there is less chance of it falling into the wrong hands. Data Secure will mask your sensitive SAP data according to security policies and rules that are delivered with the product. These rules can be extended, or new rules created to comply with company needs.

IN DEVELOPMENT ENVIRONMENT (DEV)

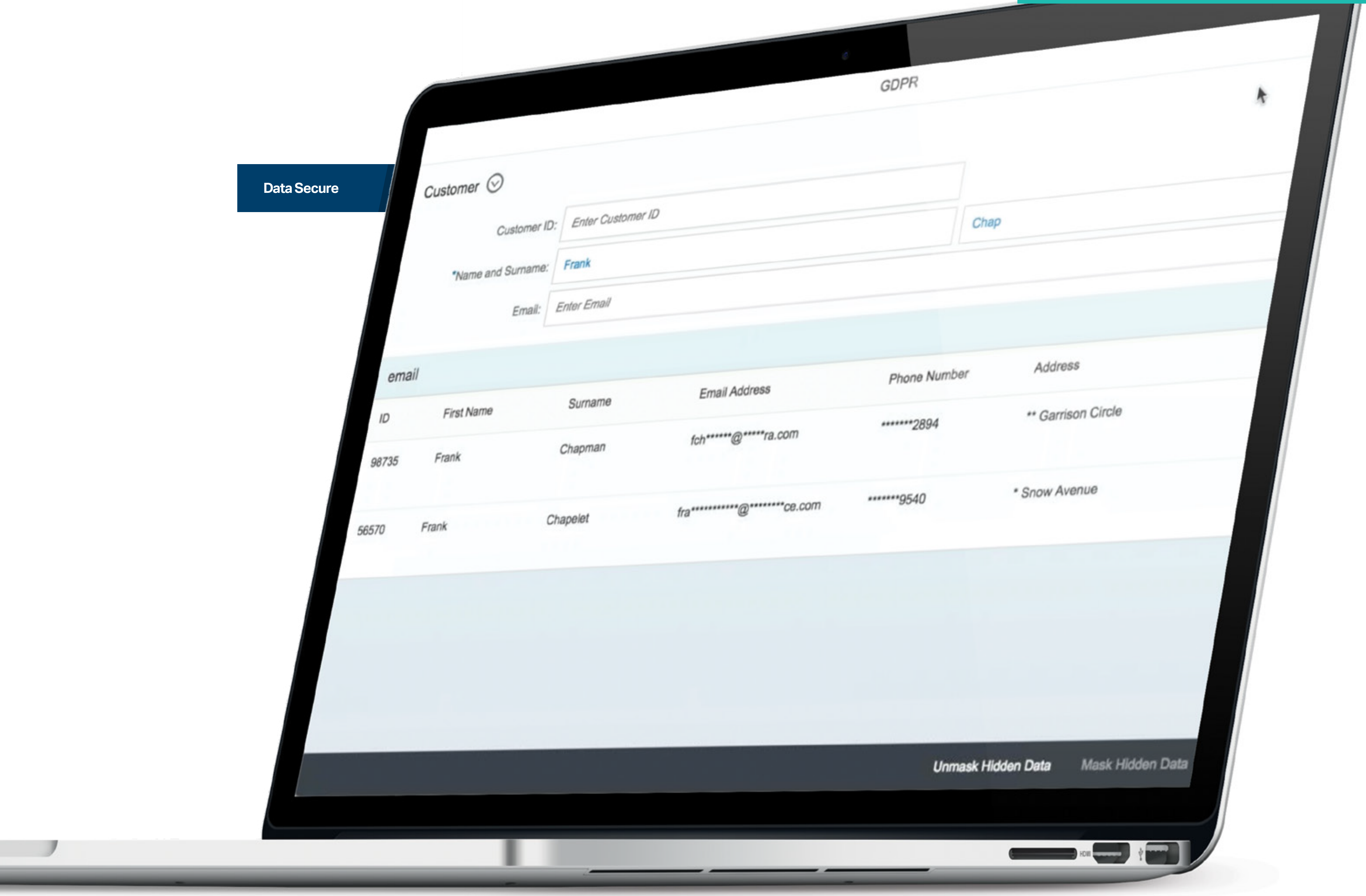
As with Quality Assurance environments, Users who have access to this SAP environment typically have more extensive access permissions. Implementing fine-grained user access in the development environment is impractical and costly. The emphasis in this environment is on basis and customization risk, and personal and sensitive data is seldom considered.

Recommended Product: **EPI-USE LABS DATA MANAGEMENT**
Relevant Module: ***Data Secure***

Data Secure is a complete data-protection solution that masks SAP data to safeguard sensitive information. Most existing data-masking solutions use "in place" masking, which means that data is masked only after it has been copied to a target system.

Data Secure takes security to a completely new level with "source-side masking". This means that the data is masked before it ever leaves the source system. The original sensitive data is never duplicated so there is less chance of it falling into the wrong hands. Data Secure will mask your sensitive SAP data according to security policies and rules that are delivered with the product. These rules can be extended, or new rules created to comply with company needs.

Data Secure



GDPR

Customer

Customer ID:	Enter Customer ID	
*Name and Surname:	Frank	Chap
Email:	Enter Email	

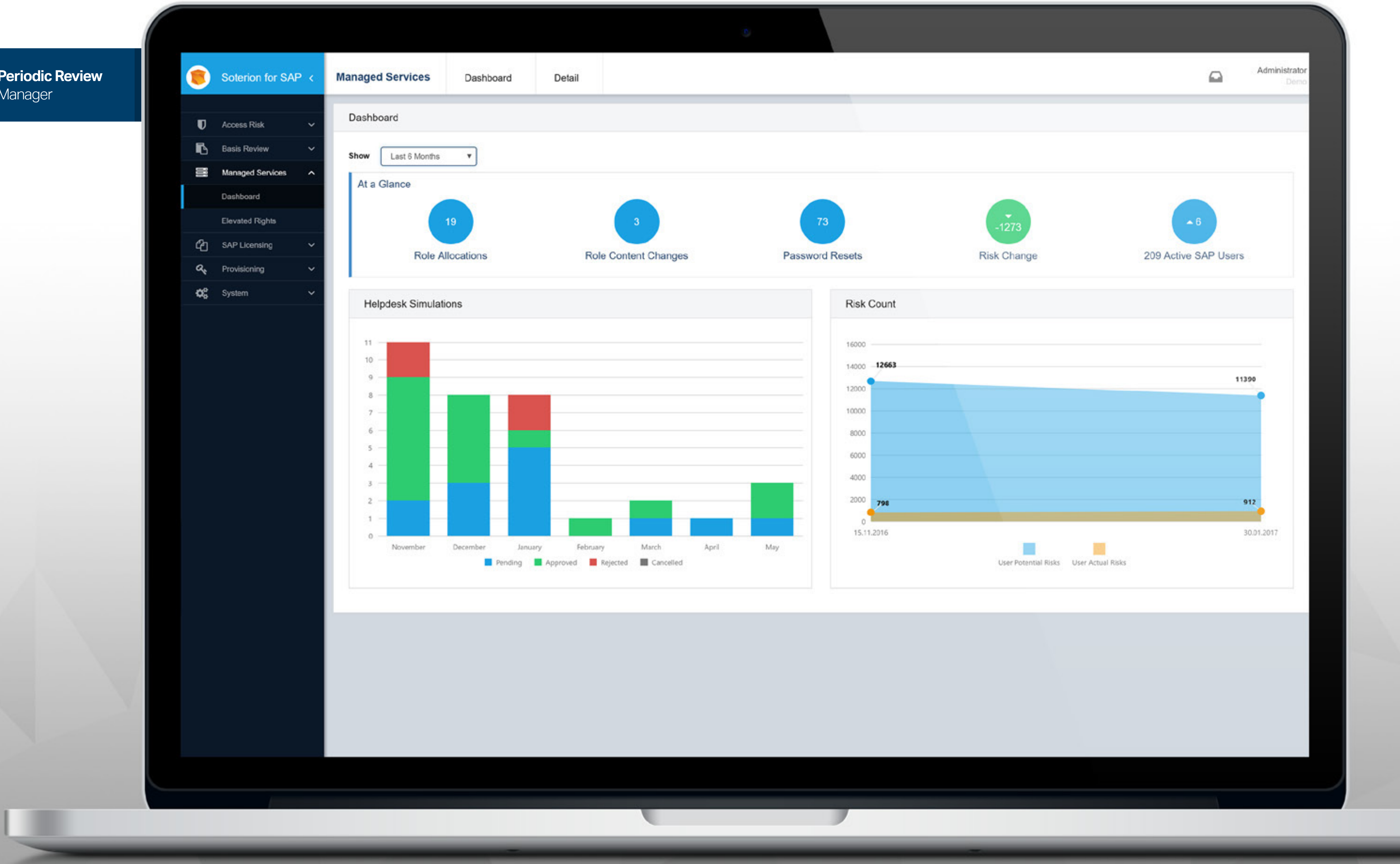
email

ID	First Name	Surname	Email Address	Phone Number	Address
98735	Frank	Chapman	fch******@*****ra.com	*******2894	** Garrison Circle
56570	Frank	Chapelet	fra************@********ce.com	*******9540	* Snow Avenue

GDPR
ACCESS RISK AND DATA MONITORING

soterion

Periodic Review
Manager



Dashboard

Show: Last 6 Months

At a Glance

19 Role Allocations

3 Role Content Changes

73 Password Resets

-1273 Risk Change

6 209 Active SAP Users

WHAT IS THIS?

After assessing your GDPR access risk and using techniques to prevent risk, the final step in the approach to GDPR compliance is the monitoring of the environments to ensure on-going compliance. User access must also be reviewed periodically to certify that the access is still relevant and necessary for processing as defined in the corporate data governance program.

HOW IS THIS DONE?

The GDPR Access Risk Rule Set and Controls must also be reviewed periodically to ensure that it sufficiently addresses the GDPR requirements for the organisation. Our solutions include tools to perform periodic reviews of User access, risk rule sets and controls. The recommended tools also supports the GDPR requirement that a data subject has the right to be forgotten.

IN PRODUCTION ENVIRONMENT (PRD)

SAP Production environments are not static, which means that both the landscape and requirements are constantly evolving. The complexity of staying compliant with GDPR legislation, and documenting compliance activities are almost impossible without a software solution.

The constant change and complexity is further compounded with challenges such as:

- ✓ Additional functionality could be introduced that is not catered for in access risk rule sets.
- ✓ Controls could be outdated or no longer relevant.
- ✓ Users may move around in the organisation and have access that is no longer appropriate.
- ✓ GDPR data subjects may exercise the right to be forgotten.

Recommended Product: **SOTERION GRC**
Relevant Module: ***Periodic Review Manager***

Data owners should periodically review which Users have access to personal and sensitive data. Since Users in SAP move through the organisation and acquire additional access, attention is seldom paid to access that needs to be revoked. The periodic review process allows business to review which Users have access to personal and sensitive data, and whether this is still relevant to the user's job function.

The GDPR access risk rule set, as well as controls, must also be reviewed periodically to assure applicability. Custom Transactions and Tables must also be assessed to identify areas where personal or sensitive data is involved.

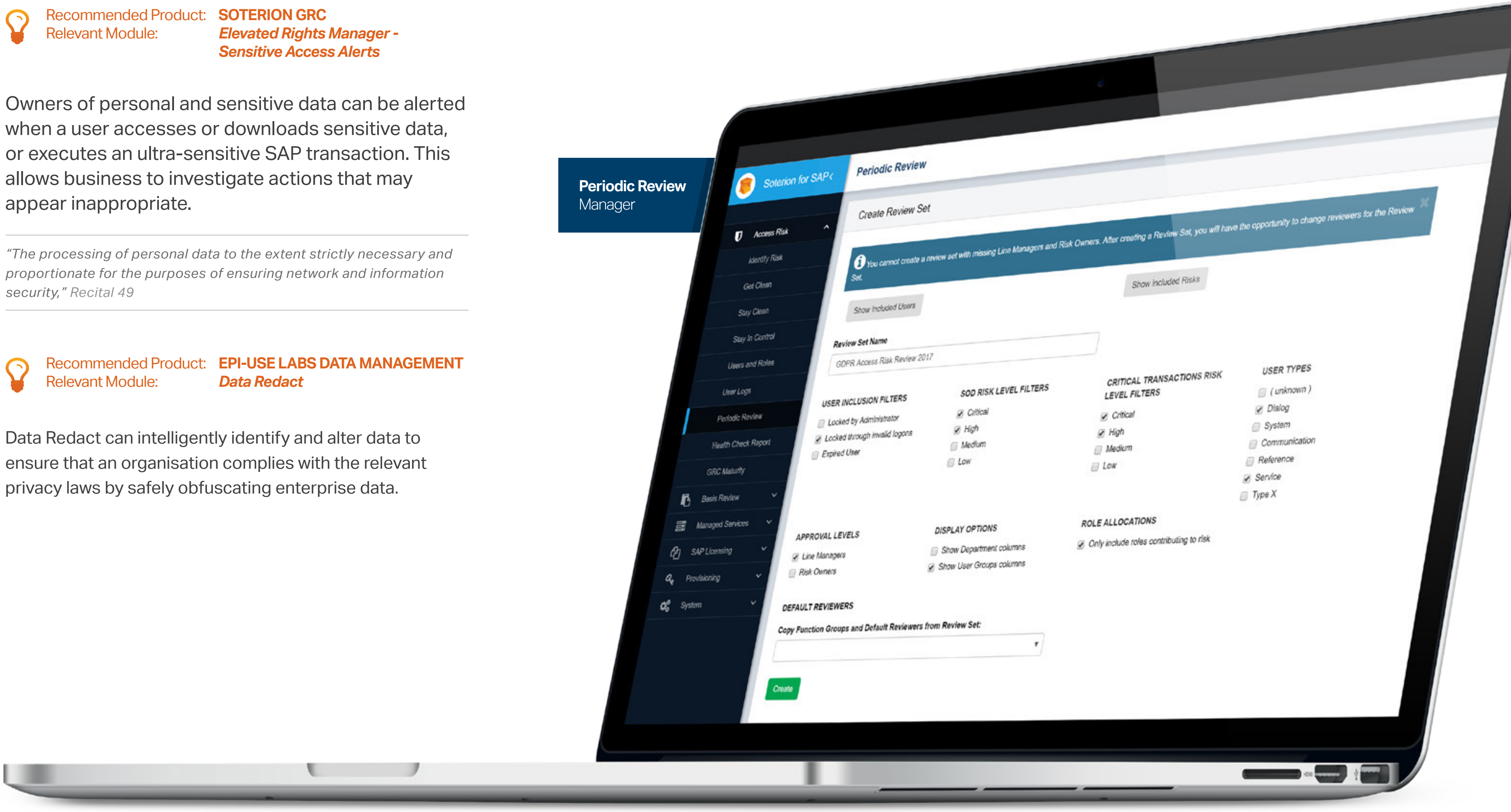
Recommended Product: **SOTERION GRC**
Relevant Module: ***Elevated Rights Manager - Sensitive Access Alerts***

Owners of personal and sensitive data can be alerted when a user accesses or downloads sensitive data, or executes an ultra-sensitive SAP transaction. This allows business to investigate actions that may appear inappropriate.

> *"The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security,"* Recital 49

Recommended Product: **EPI-USE LABS DATA MANAGEMENT**
Relevant Module: ***Data Redact***

Data Redact can intelligently identify and alter data to ensure that an organisation complies with the relevant privacy laws by safely obfuscating enterprise data.



Periodic Review Manager

Periodic Review

Create Review Set

You cannot create a review set with missing Line Managers and Risk Owners. After creating a Review Set, you will have the opportunity to change reviewers for the Review Set.

Review Set Name: GDPR Access Risk Review 2017

USER INCLUSION FILTERS
□ Locked by Administrator
☑ Locked through invalid logons
□ Expired User

SOD RISK LEVEL FILTERS
☑ Critical
☑ High
□ Medium
□ Low

CRITICAL TRANSACTIONS RISK LEVEL FILTERS
☑ Critical
☑ High
□ Medium
□ Low

USER TYPES
□ (unknown)
☑ Dialog
□ System
□ Communication
□ Reference
☑ Service
□ Type X

APPROVAL LEVELS
☑ Line Managers
□ Risk Owners

DISPLAY OPTIONS
□ Show Department columns
☑ Show User Groups columns

ROLE ALLOCATIONS
☑ Only include roles contributing to risk

DEFAULT REVIEWERS
Copy Function Groups and Default Reviewers from Review Set:

CONCLUSION

Even though the requirements to work towards GDPR compliance can be daunting, it is a reality that will need to be addressed as a matter of urgency. The key factors are to remain pragmatic and to introduce these concepts gradually and intentionally by using the proposed methodology as outlined in this document. This methodology which was developed specifically to assist an organisation to ensure that the required controls are adopted effectively.

Our multi-phased approach combined with the suggested technologies available from Soterion and Epi-Use Labs will allow for each challenge to be addressed sequentially while managing the risks in each SAP tier and complying with demanding time frames.

WHO IS **SOTERION**

We specialise in helping companies maximise their Governance, Risk and Compliance (GRC) processes. We understand the unique opportunities and challenges that exist at most corporates when it comes to their GRC capability.

Many feel overwhelmed and intimidated by SAP GRC and its seeming complexities and expenses, and hence they are hesitant to even begin the process. Others may feel like they're not seeing the full benefit of their SAP GRC software.

With an aim to get our customers to view GRC not as a burden, but as a real benefit, we've developed a number of niche GRC tools. Brought to you by our team of expert consultants situated around the world, we specialise in demystifying, uncomplicating and expediting the GRC process.

We Solve GRC for SAP Companies

Software-as-a-Service

What is it?

Soterion's Compliance Cloud platform is a cloud based, pay-as-you-go GRC Access Risk tool.

Ideal for?

- Highly cost-sensitive companies.
- Companies that require access risk assessments seldom or ad hoc, for example: internal auditors.
- Companies with basic in-house GRC expertise.

Benefits

- Instant GRC access risk visibility
- Easy-to-use
- Business-friendly reporting
- Extremely cost effective
- Only pay when you use it

Managed Service

What is it?

Combine 'on-tap' GRC expertise with Soterion's Compliance Cloud platform for a complete GRC solution. Delivered in collaboration with Soterion's Consulting Partner Network.

Ideal for?

Companies who have a GRC requirement, but lack internal expertise.

Benefits

- Instant GRC capability, including both tools and expertise
- Give business hassle-free, complete control of access risks via dependable GRC service
- Significantly cheaper overall solution than employing in-house GRC expertise and purchasing GRC tool
- Proactive GRC management

On-Premise Software

What is it?

Soterion for SAP is a size-sensible GRC software application, offering powerful, easy-to-use features for SAP companies.

Ideal for?

- Companies that have a GRC requirement, and have internal expertise.
- Companies with IT policies requiring on-premise solutions.

Benefits

- Powerful, size-sensible GRC features for smaller businesses without complex, unnecessary functionality
- Highly cost-effective on-premise GRC alternative
- Intuitive and easy to use
- Minimally invasive to infrastructure and SAP installation

AUSTRALASIA

Levels 5 & 6,
616 Harris Street, Ultimo
NSW 2007

Tel: +61 4 1067 9981

ASIA PACIFIC

1 Fullerton Road
#02-01 One Fullerton
Singapore 049213

Tel: +65 6650 5294

SOUTH AFRICA

Block A, Wedgefield Office Park
17 Muswell Road
South Bryanston
Johannesburg 2021

Tel: +27 11 540 0232

THE NETHERLANDS

4 Polanen street
Nieuw-Vennep
2151DP

Tel: +31 61 105 6891

info@soterion.com www.soterion.com

soterion