SAP and GDPR:
Keeping Your Organization Ahead of the Upcoming EU Law

Introduction

With each passing year, the information age becomes even more digitalized. Almost every process from shopping to healthcare, in one way or another, demands the handover of digitized personal data into the care of those who promise to handle it responsibly. With the submergence of society under the digital wave of the new millennium this data might rapidly be drifting out of reach. Out of reach and into the nets of those that treat it like a commodity or worse.

In an attempt to give back the control of their personal data to its citizens, the European Union (EU) has drawn up a modernized law to protect that data: the General Data Protection Regulation (GDPR). GDPR provides a legal framework for compliance, affecting global businesses with headquarters both inside and outside Europe. The official GDPR regulation can be found on the EUR-lex website. This robust policy has a firm deadline of the 25th of May 2018 with severe fines facing organizations that are not in compliance.

This whitepaper strives to provide structure to the 88-page legislation by separating it into smaller segments for SAP customers to be able to answer a few of their most important questions. The first section of the whitepaper will be valuable for anybody wondering if they are affected by GDPR as it will go through the regulation at a high level. We will then focus on SAP itself and how to approach the challenge of making sure that your systems are compliant. A large part this whitepaper will benefit anyone looking for a hands-on approach to achieve GDPR compliance from a more technical system analysis perspective.

What is GDPR?

The EU considers data protection of its citizens a fundamental human right. It acknowledges that the advancement of technology and globalization have been factors contributing to the proliferation and ubiquity of data. In the words of GDPR:

> *[…] rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. (Recital 6)*

Technology is causing citizens to lose control of their data. Currently in the EU, there are no mandates that keep track of the travel of data, let alone existing means to retrieve or delete the data. According to the EU, “the processing of personal data should be designed to serve mankind solely,”[1] which means regulations need to exist. GDPR, replacing Directive 95/46/EC, was adopted on the 27th of April 2016 and is in a two-year transition period before the looming enforceable deadline of May 2018.

Adopted in 1995, Directive 95/46/EC was a set of objectives and principles guiding EU member states to create and implement their own mandates regarding data protection. This directive led to the creation of individual member state laws. The United Kingdom’s *Data Protection Act 1998* is an example of such a local law. The Dutch *Wet bescherming persoonsgegevens* is another. GDPR repeals Directive 95/46/EC and transfers control of legislation out of the hands of individual member states into those of a centralized body. The GDPR legislation thereby not only promises to provide freedom, security and justice to the Union, but also to unify regulation in order to provide more clarity for parties seeking compliance. The fragmented nature of the previous separate member state laws caused confusion and hesitation for companies involved in cross-border processing, i.e., ”the processing of personal data, which takes place in the context of the activities of establishments in more than one Member State.”[2] An intended *one-stop-shop* mechanism claims to relieve businesses of the legal and compliance worries accompanying cross-border flows of data. Granted, these worries may be replaced by others concerning hefty sanctions if failing to comply. Some examples:

- *Administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. (Article 83, Paragraph 4)*
- *Administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. (Article 83, Paragraph 5 & 6)*

Does it Apply to Me?

Regardless of your company’s headquarter location; if you are processing EU citizens’ personal data on a regular basis then most likely GDPR applies to you.

***Personal data** means any information relating to a [...] natural person (‘data subject’); [...] to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Article 4, Paragraph 1)*

Some examples of personal data are obvious: a name, social security number or email address are just a few examples; but, how about resumes, employment history, health data, tattoos, scars, DNA or fingerprints? According to GDPR, these also qualify. Less obvious, however, is data that seemingly does not concern a person but can be reasoned back to a data subject with a bit of forensic puzzling. This means data like IP addresses and URLs might qualify as personal data in the context of GDPR.

For example, let’s consider customer data as a form of personal data for a moment. If your customers are European citizens, their personal data will very likely be processed or retained on your SAP systems. A customer’s postal or email address already qualifies for the above definition. If your company is the one

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679
[2] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

determining the purpose and means of the processing, then your company is considered a *controller* in GDPR terms. The controller can send personal data to another company for further processing. This company is called a *processor* in GDPR terms. Processors and controllers established in the EU or processing EU citizen personal data are bound under GDPR. However, non-EU based companies should also be concerned. Even though they may be located outside the EU, they are considered a part of GDPR when they are performing the following activities:

> *a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
>
> *b) the monitoring of their behaviour as far as their behaviour takes place within the Union. (Article 3.1)*

Even if both controller and processor are established outside the Union, GDPR could apply in the above cases. Firm agreements and clear lines of communication need to be in place between processors and controllers. Accountability for the location and life span of every piece of personal data needs to exist.

Players

A few main players within the field of GDPR have been previously mentioned. The *controller* decides why and how a *data subject's* personal data is processed. A controller might delegate further action to a *processor*. Your company may be one of these two players, or both. Any other party authorized by the controller/processor to process data is referred to as a *third party*. Figure 1 conveys all players involved in GDPR compliance and their relationship to each other.

Supervisory Authority

To enforce GDPR, more players will likely be involved. The most important of which is the *supervisory authority (SA)*. Each EU member state will supply, equip and finance an SA (although SA's are required to operate in independence and secrecy). These SA's will monitor companies to confirm correct application of the GDPR in each member state. Compliance will need to be demonstrated to these entities. For a controller or processor, the *lead supervisory authority* is the SA in the member state of its main establishment. This SA will be its approachable link to law and law enforcement in case of compliance queries, audits and data breaches. In the case of a company's establishment in multiple member states, the SA's of the member states will report to the lead SA, thereby centralizing control. This hierarchy aims to constitute the one-stop-shop mechanism mentioned previously.

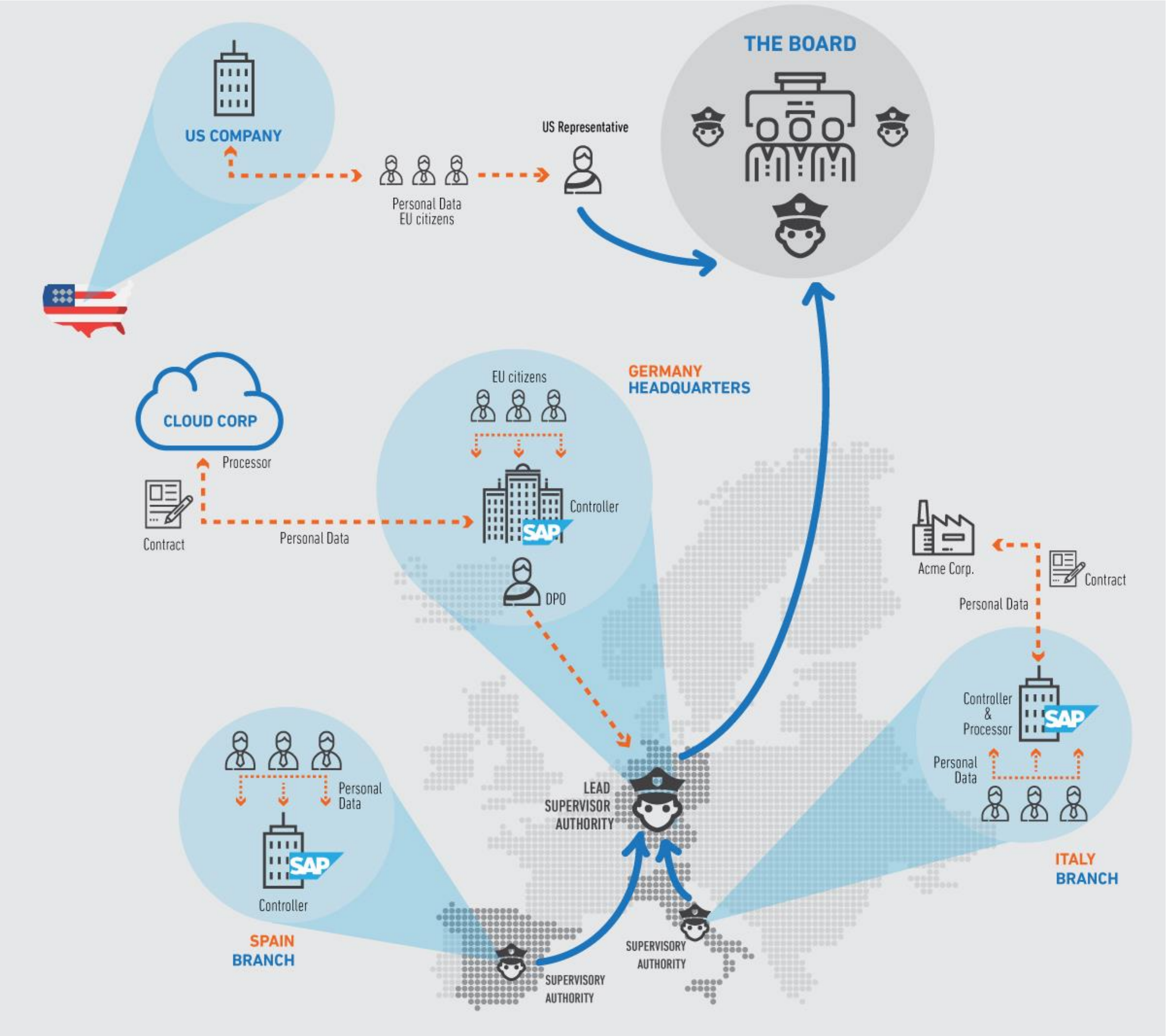


Figure 1: Players within the field of GDPR

Data Protection Officer

In certain cases, the controller/processor shall appoint an independently operating *data protection officer* (DPO). The DPO will be working in-house, independently, to inform and advise the business on compliance issues. The DPO also acts as a contact point for both citizens and the supervisory authority.

GDPR does not describe in a clear way which companies are required to assign a DPO, since not all of them do. The scale, repetition and nature of the processing operation plays a part in the decision. You may choose your own DPO if you determine that you need one.

Representative

Where a controller or a processor not established in the EU is processing personal data of subjects inside the EU and needs to comply with GDPR, the controller/processor should designate a *representative* in the EU. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate from the controller or processor to act on its behalf with regard to its obligations under this regulation. The representative will play an enforcing role for non-EU-based controllers/processors.

The Board

The main authority holding the book of rules is the *European Data Protection Board*, also referred to as *the Board*. The Board, represented by the *Chair*, is composed of the heads of all member state SA's. The Board is the final manager ensuring GDPR is applied properly.

Key Aspects

The GDPR policy intends to guard the three principles of *lawfulness, fairness and transparency* in relation to personal data. This means a valid reason should exist, in proven writing, to process personal data, in conjunction with plans to retain that data. Processing data outside the specification of purpose is prohibited. The same goes for processing the data within the specification, yet taking longer than necessary to do it. Data being retained within the boundaries of purpose is required to remain accurate and up-to-date. Technical and organizational means to ensure the integrity and confidentiality of remaining data should be in place. In addition, these need to be communicated clearly to data subjects.

The three principles of lawfulness, fairness and transparency connect to specific rights for EU citizens, concerning their data. Rights guaranteed by those processing the data are:

- Every data subject needs to give consent to the processing of its data. This consent needs to be explicitly requested, explicitly given and registered for later demonstration. The consent can be withdrawn by the data subject at any moment. In the words of GDPR, "it shall be as easy to withdraw as it was to give consent."[3]
- Every data subject has the right to know where its data is being processed, what is being processed and why.
- Every data subject has the right to obtain the data without delay and to demand it erased immediately (*right to be forgotten*).
- The data subject has the right to demand rectification of data and the right to object further processing of data.
- Every data subject has the right to request the movement of its data to a different controller (*right to data portability)*. After which the data should be presented in a neat, structured and machine-readable format by the current controller. If technically possible, the data should be able to be transmitted directly to another organization of choice.
- Also, the data subject has the right not to be subject to decisions based solely on automated processing, including profiling (i.e. a*utomated processing to evaluate personal aspects relating to the data subject*).

[3] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

The rights stipulated above alone will lead to significant challenges for controllers. Additionally, since data subjects might not be aware of these rights, their rights should be communicated to them clearly whenever an exchange of personal data is about to be made. No assumptions are to be made; full transparency is required. Records of the whereabouts of data should be kept. At any time, for every piece of personal data, it should be known where the data is retained, where it will be going next and especially why. These factors are to be considered, put in writing and communicated when requested.

Contracts or legal acts should exist between controllers and processors, describing all data flows to always facilitate the right for a data subject to have insight into the process. A contract should set out "the subject matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject."[4] Furthermore, a controller will not be allowed to contract just any processor. Only processors that can demonstrate their technical and organizational expertise and have the resources to comply with GDPR are to be considered.

GDPR dedicates a full article to the principle of 'data protection by design and by default'. This principle essentially directs organizations to build measures of safeguarding data protection into the design of technical and organizational processes from their very conception, ahead of the actual processing. The default setting for every newly spawned business process should be focused on data protection and the minimization of processing of personal data. Some important technical measures are, for instance, data *pseudonymization* and encryption.

> *[…] the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. (Article 25.1)*

Prior to even starting to process personal data, those companies in high risk of violating the rights and freedoms of data subjects are required to perform a Data Protection Impact Assessment (DPIA). The DPIA shall be executed in close cooperation with a DPO. It shall describe the processing, its purpose, the necessity of handling the personal data, a description of risks in relation to rights and freedoms involved and how to address these risks. Seeking the views of data subjects on these topics might even be necessary. A changing environment, with recalibrated risks, will require a revisional impact assessment.

Data breaches should be rapidly communicated to SA's *and* data subjects.

> *'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. (Article 4)*

No later than 72 hours after having become aware of it, a data breach should be reported by a controller. According to the legislation, "where such notification cannot be achieved within 72 hours, the reasons for

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

the delay should accompany the notification and information may be provided in phases without undue further delay."[5] A data breach should not only be reported to the SA, but also to the data subject involved (certain conditions apply). Exceptions apply, for instance if breached data is rendered unintelligible by means of encryption. If a controller is not communicating with the data subject to the SA's satisfaction, the SA may choose to do so in its place.

This last point may seem obvious, but the bright side is that the Union intends to reward parties who have been able to show compliance with *certifications, seals and marks*. This means you will be able to distinguish yourself from others who have not been able attain certification, which could drive possible customers in your direction, or at least help to reduce the pool of competitors in your market.

Road to Compliancy

It is almost certain GDPR will have an impact, in some way or another, on any company large enough to have chosen SAP to run its business processes. GDPR will touch multiple areas of this type of organization, far from solely the technical one. Because of this, GDPR should not be underestimated, although signs are showing that companies have been ignoring this until now. These companies are starting to realize that gearing up for GDPR will not be a mere tweak of the current company privacy policy, but rather a complete overhaul of existing business processes.

Getting in line with GDPR involves setting up a multidisciplinary team and beginning a readiness plan to work on a specific GDPR compliance program. The legal team may need to get started on third-party contracts, not to mention the interpretation of the actual regulation. The security department should decide on their data breach scenarios or better yet; what needs to happen to stop breaches from happening in the first place. Human resources might want to dig into the archives to see what information can be removed and which members of the team will redesign business processes and communication flows. Also, the IT department should get started on an in-depth analysis of the information environment.

The road to compliance starts with a full assessment of the current state of affairs. If previous data privacy practices are already in place, that might be a good place to start. If not, the workflows inside all sections of the business need to be accurately analyzed, described, possibly redesigned and followed up on with GDPR in mind. Communication flows, within the organization, towards partners, customers and government regulators need to be specified. Companies should educate employees on these new processes through trainings. Consent mechanisms will need to be in place (and stored for future reference), which give data subjects the opportunity to proactively opt into handing over their data.

Ultimately, compliance will need to be proven. Organizations will need to set up an audit and compliance governance structure, possibly under direction of a DPO, who will be reporting to supervisory authorities. That privacy governance structure would be set up to stay, since proving compliance will become a reoccurring event within the company.

The analysis of personal data flowing through your SAP landscape will be one of the tasks at hand. The sections below intend to offer suggestions on where and how to start on that task.

[5] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679

SAP and GDPR: Where to Start?

There are many angles to consider when building a readiness plan to attack GDPR compliance, which could lead to many organizations struggling with where to even start. A majority of SAP users are feeling distressed when thinking about the magnitude of the challenge. For example, research conducted by the UK & Ireland SAP User Group shows 86% of SAP users[6] do not fully understand how GDPR will affect their SAP landscapes and how to reach compliance. The product is so complex and customized, with so many moving parts, that the best strategy is to begin by finding an abstract model that simplifies the discovery of personal data. In this section, we intend to do exactly that.

By creating a conceptual model of the product, we are providing a high-level overview, enabling you to start the process of understanding if personal data exists in your SAP environment. While it may be impossible to find every location the data is stored, and what type of data it is, this exercise will at least help you understand if GDPR is something you need to be concerned with.

Let's start with GDPR's core element: personal data. If you discover that your organization does not handle EU citizen's personal data you can move on with confidence that GDPR will not apply to you. The first question to ask therefore is: does my organization even handle personal data at all? An interesting exercise to discover this would be to consider all workflows within in your organization and to see where the concept of personal data comes in.

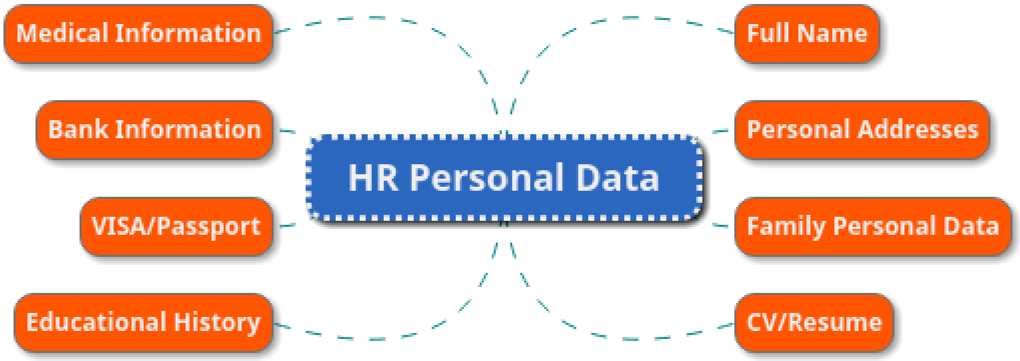


Figure 2: Personal data in an HR workflow

Let's take Human Resources as an example. Recruitment, hiring, employment and termination of employees are all phases found within a typical long-term HR workflow. Figure 2 above shows some of the personal data involved, starting from the first contact of a prospective employee (GDPR data subject) until the moment he or she leaves the company. During all phases, personal data might be flowing through the organization ubiquitously. During recruitment, names, email addresses and phone numbers are registered. While hiring, medical/psychological background data, banking data and contract data may be stored. During employment, travel may require saving passport and family data. The employee may also obtain certifications of which you may register the license ID's.

[6] http://www.itpro.co.uk/it-legislation/28840/users-fear-sap-systems-make-gdpr-compliance-harder-to-achieve

Has your organization thought about what happens to all this data (or where it remains) when the employee leaves the company? And, to put this challenge into perspective, this is just one of many business workflows that organizations run in SAP.

Knowing which personal data exists within your organization, how it got there, and where the data is stored is essential. Next, it will be important to find out and limit who is authorized to access this stored data and even *how* the data is being stored. In other words, can the data be stored encrypted or pseudonymized to essentially limit access for less authorized users? This goes for all parts of the organization; however, in this paper, from here on out, we will be looking at this from an SAP perspective.

Abstraction of the SAP Landscape

We need to develop a critical eye towards pinpointing personal data, how it arrives, where it goes, where it is retained, how it is retained and who can access it. The following model applies:

Viewing SAP through GDPR glasses, while focusing around personal data, we can construct a multi-layer model, as seen in Figure 3. From top to bottom:

- The **Interface** Layer: This is the SAP user-interfacing layer. It is the layer through which personal data first enters the SAP environment and the layer that presents a way to interact with personal data, often in a human-friendly format. It is also the layer through which that personal data may be altered and finally deleted. Basically, it is safe to say that if any personal data exists or is flowing through the SAP system, it has entered through the data interface layer.

- The **Solution** Layer: The solution layer is the semantic layer. It determines whether data entering through the interface layer could indeed be personal data. For instance, the human capital management (HCM) module facilitates data as discussed in our workflow example: names, addresses and medical data of employees. What types of personal data are contained within the system is determined by this layer.

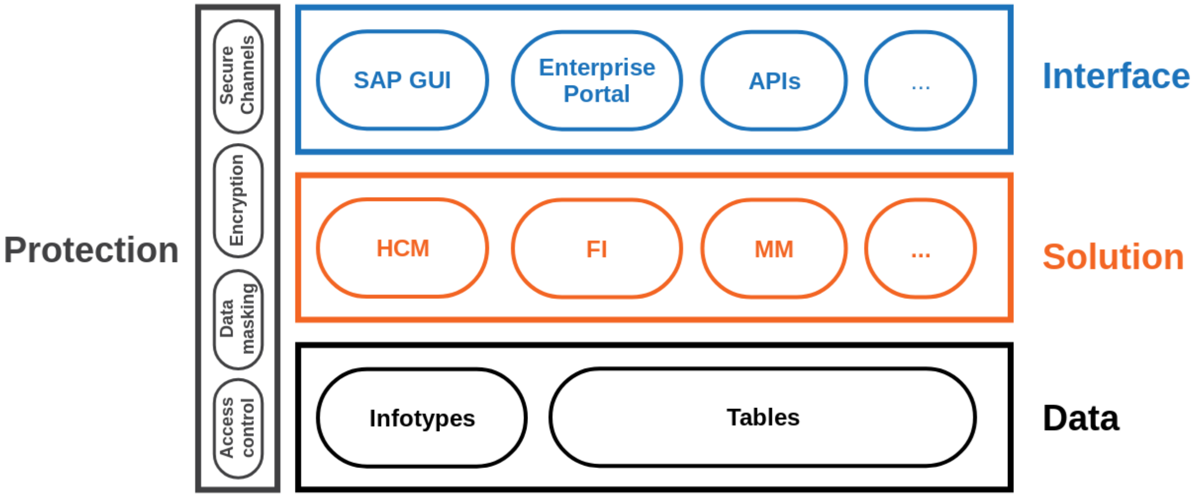


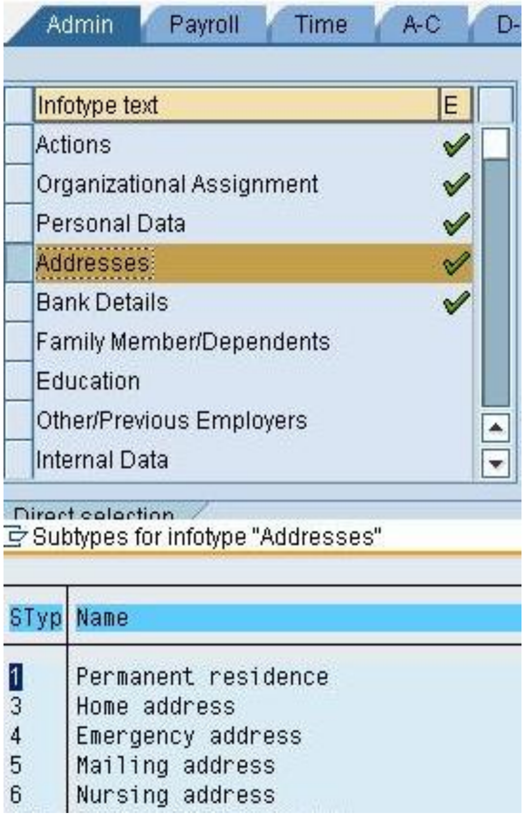
Figure 3: SAP abstract data model

- The **Data** Layer: The data layer handles the retention of personal data in elemental units. Data flows into the model from top to bottom and in this layer the data is retained. The solution layer will determine the type of elemental unit (infotypes, tables) and the semantics of that elemental unit (i.e. whether the unit contains personal data).

- The **Protection** Layer: The vertical protection layer encompasses the previously mentioned four layers. It determines the form in which data is retained or presented. The form or way in which data is retained is highly important in light of GDPR. Different protection techniques exist: encryption, data masking (pseudonymization) and access control. Every technique provides steps in the right direction for GDPR compliance. These functions can be approached on different horizontal layers within the model.

In the following sections, we will go through the layers in our suggested model, starting with the solution layer. The idea is to use the abstract model to provide an approach, rather than concrete instructions. Although some examples will be used to illustrate our points, it would be impossible to describe the exact path to compliance considering the extensiveness of SAP. Dozens of modules and solutions, thousands of tables and more than a hundred thousand transactions will require you to create your own custom approach. Dividing the challenge into these abstract building blocks might help you.

Solution Layer



Infotype text	E
Actions	✓
Organizational Assignment	✓
Personal Data	✓
Addresses	✓
Bank Details	✓
Family Member/Dependents	
Education	
Other/Previous Employers	
Internal Data	

Subtypes for infotype "Addresses"

STyp	Name
1	Permanent residence
3	Home address
4	Emergency address
5	Mailing address
6	Nursing address

Figure 4: Infotype "Addresses" in HCM

The SAP modules running within your company will determine which components within each abstract layer require attention. For instance, the HCM module will lead to the use of infotypes in the data layer as seen in Figure 4. Also, using HCM means you will interact with the data through a defined range of possible UIs on the interface layer. You will need to go through each solution running within the company and map which components within each layer apply to that solution. Viewing the layers in the model on a per solution basis narrows down the search for personal data, simplifying the challenge as you go. In that sense, the solution layer is a good starting point for analyzing the more low-level details of your SAP system.

Starting from the solution layer could also be useful for analyzing the rest of your organization from a higher level. In the previous exercise you will have already tried to picture the workflows within your company. As you go through those workflows, try to see where they coincide with the SAP modules in operation. The parts of those workflows *not* performed through SAP can indicate where SAP meets non-SAP business processes in your organization.

Following the HR workflow example, SAP's human capital management (HCM) is a module used to perform a major part of HR tasks. This module is used to manage the *people* in an organization and therefore indicates a high probability of personal data being handled. Therefore, HCM is a prime suspect to take into account. However, be aware that less obvious modules referencing personal data exist. Materials management (MM) contains customer and vendor data. Financial accounting (FI) will link to similar data such as bank accounts and credit card numbers.

Asking yourself which departments interact with which SAP modules could be a useful starting point to answer some crucial questions:

1. Who is accessing the system?
2. Do these people have a direct need to access the system?
3. In what manner could data proliferate outside the SAP landscape, due to specific people accessing the system?
4. Could this need to access the system be delegated to others also accessing the system (thus limiting the access)?

One could say the solution layer is where SAP connects to other non-SAP business processes inside your organization. Viewing GDPR from an organizational level, the solution layer is the connection point between SAP compliance and compliance of the organization as a whole.

Data Layer

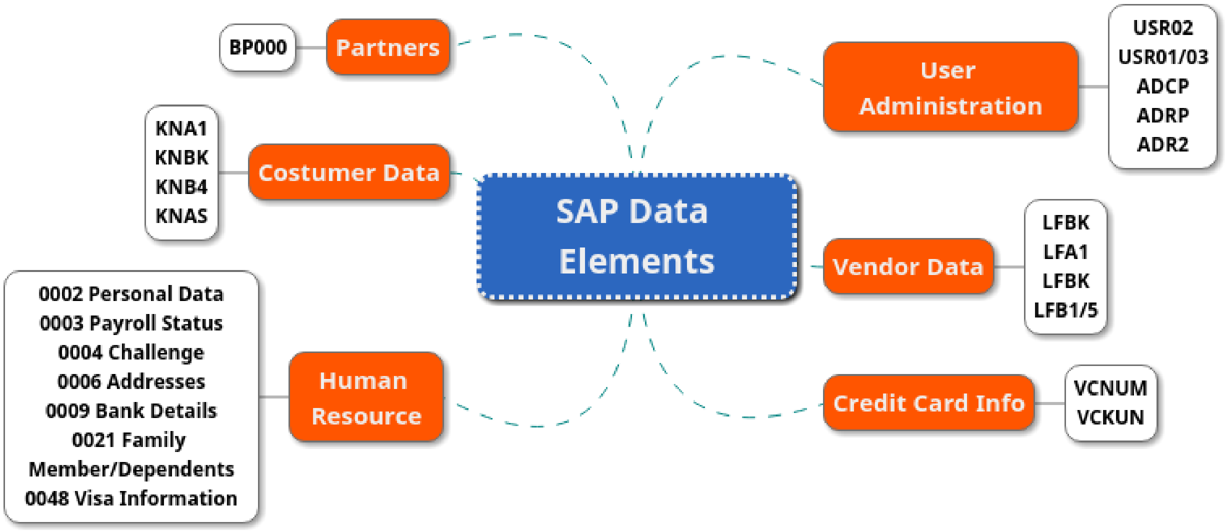


Figure 5: SAP data elements per category

Depending on the SAP module under scrutiny, personal data may be stored in different elemental units. In a broad sense, the data layer elements typically will be SAP tables. First determine which tables store personal data, then, decide if the data needs to be there and how to get it under control. Depending on the module under consideration, this could be the table ‘VCNUM’ that stores credit card data, the ‘KNA1’ table for customer data or the table ‘LFBK’ for vendor data, amongst many others. More examples of elementary units containing SAP data can be found in Figure 5. The essence is, that in view of the data layer, we need to identify all personal data units for all modules and critically assess, with the regulation in mind, whether this data is considered personal data under GDPR. After finding the most elemental units storing personal data on the data layer, we can limit access to them through the protection layer.

In the HCM module personal data is stored in infotypes. A typical infotype (006) can contain address information, including a range of subtypes like home address, mailing address and more. Other infotypes could be bank details (009), contract elements (0016) or internal medical service (0028). The goal is to identify which infotypes are used in your organization in the case of the SAP HCM module.

To find all tables of interest you can go to transaction 'SE11' and select the 'DD02L' table in the *database table* field. In the dialog box that appears, choose *SAP applications*. After that you can browse tables categorized by application components.

Interface Layer

Knowing how users interface with your system is important, since it will provide you with a defined scope of how data enters the system and ends up in the data layer. Controlling access, organizationally and technically, can reduce that scope. Reducing scope is a movement towards GDPR compliance.

Advanced business application programming (ABAP) systems are managed by the SAP GUI. In general, when considering ABAP, the data in the data layer will interact through transactions. Many transactions exist and many relate to personal data. An example is 'SU01'; a user data transaction which allows you to maintain users. Speaking generally, the users of your SAP system, where personal data is a concern, could range from partners to external consultants to customers. Personal data entered through 'SU01' may consist of a first and a last name, telephone number or department. This user data is written to and read from the tables discussed earlier. 'USR02', for example, contains user name as well as *valid from* and *to* dates. Other transactions used for personal data are 'SU10' (user maintenance: mass changes) or 'PA40' for personnel actions in the case of HCM. Choosing which transactions are assigned to which users helps narrow the scope of GDPR.

Java systems will interface with personal data by using identity management in SAP Netweaver Java or by using the Visual Administrator. However, if you are only considering the out-of-the-box graphical UI's provided by SAP, you might be overlooking things. SAP is renowned for providing rich building blocks used by developers to create their own applications and interfaces to interact with data. Examples of this could be Business Server Pages (BSP) which enable SAP applications to be displayed via an HTTP connection using a standard browser or the many APIs[7] offered by SAP. Knowing which custom applications you are running and who has access to them is an important step.

Protection Layer

After you have determined which personal data has qualified and will remain in the system, your next task for compliance will be to take measures in the protection layer. This layer cannot effectively be placed horizontally, in between the others, because it encompasses multiple layers.

Authorization and Access Control

Make sure you know who can access personal data and try to limit who can access that data. In other words, perform tight access control on your personal data to reduce the field to which GDPR applies.

[7] https://api.sap.com/shell/api

Review your user master records and gain insight into who has access to the system, their assigned roles and thus which transactions they can execute. By using transaction 'PFCG' in ABAP systems, you can maintain roles, authorizations and profiles. The basic workflow should be:

1. Think about which transactions are needed by the different departments within your organization.
    a. Be sure to consider segregation of duties (SoD), by assuring no single individual has access to all business processes.
2. Bind these transactions together in roles, where roles represent the organizational plan of your company.
3. Edit the profiles belonging to the roles. The profiles will contain the authorizations by connecting authorization objects. Avoid or eliminate the use of the 'SAP_ALL' and 'SAP_NEW' profiles.
4. Edit authorization objects by linking fields with permitted activity here and connecting them with profiles.
5. Assign users to the roles. Limiting the number of users will help shrink the scope of GDPR.

Authorized users are authenticated by their credentials. Review your password policy, for it will prohibit this from becoming the weakest link in your protection scheme.

Developers working on your SAP environment pose an additional risk for compliance. Review who they are and what they should be working on. Check who is currently in possession of development keys. By using table 'DEVACCESS', you will get an indication of who has or once had access to the system objects as a developer. It is important to note that a removed development key will still allow the original assignee and if his or her authorization has been altered.

Encryption

Strongly encrypted data is useless to attackers in the case of a data breach. And thus, encryption might save you much needed time, effort and reputational damage if your organization is compromised. It also might dismiss the need to communicate the breach to the data subject, as instructed by GDPR.

Encryption happens on, or, technically speaking, below, the data layer. In SAP, it is accomplished through SAP SSF[8], the secure store and forward interface (BC-SEC). In the context of SSF, you will need to use the SAP cryptographic library for encrypting data in the system. After installing this function package, a public-private key pair needs to be generated and stored in what SAP calls a personal security environment (PSE).

The next steps will be specific, depending on the module in use. For example, encrypting credit card data in the HCM module has its own specific workflow. In this case, in order to migrate unencrypted database entries to encrypted storage, or vice versa, the migration program 'RCCSEC_MIGRATION_070' is delivered. Following the documentation will provide you answers for each specific situation that is relevant to you. SAP notes #662340 and #1059333 exemplify this.

Secure store and forward (SSF) ensures integrity and confidentiality of data by wrapping data and documents in digitally signed "envelopes" for secure storage and transmission. The data remains secure, even after exporting it out of the system. SSF can provide your organization with tight control over the

[8] https://help.sap.com/saphelp_nw74/helpdata/en/53/251a355d0c4d78e10000009b38f83b/frameset.htm

identification and origin of data, who can and cannot see data or whether data may have been tampered with (data breaches).

The HANA database, although running in memory, will be saved to disk at regular intervals. For example, deltas are saved into the redo-log on disk. Not to mention data and log backups. Encryption, next to authorizations, adds an extra layer of protection here. In HANA encryption of the data area, a redo-log area and backup area exists. Applications requiring encryption use the internal encryption service. Check the SAP HANA Security Guide for more detailed information.

Masked Display (Pseudonymization)

Where personal data needs to be viewed by people with different degrees of authorization, masked display, or pseudonymization, can offer an easier way to obscure sensitive data for unwanted eyes. This limits the scope of personal data. Pseudonymization in GDPR terms means that the system hides part of the number when displaying or changing objects. For example, in the case of a payment card number, the system can display the value ‘1111********4444’ instead of the card number ‘1111222233334444’ as seen in Figure 6. You can set the number of visible characters at the start and end of the payment card number. Again, how to technically mask the data will be entirely specific to your situation. The SAP knowledge base should again provide answers to this.

Data masking in SAP HANA happens at the database level, where specifically chosen queries determine how data is represented. Therefore, in HANA, data masking is not an interface, but rather a data layer feature. The following view definition shows how data masking in HANA may work. The view specifies how the column should be returned by referencing a mask expression:

```
CREATE VIEW <view_name> (<column_name_list>) AS <subquery> WITH MASK
(<column_name> USING '<mask_expression>’);
```

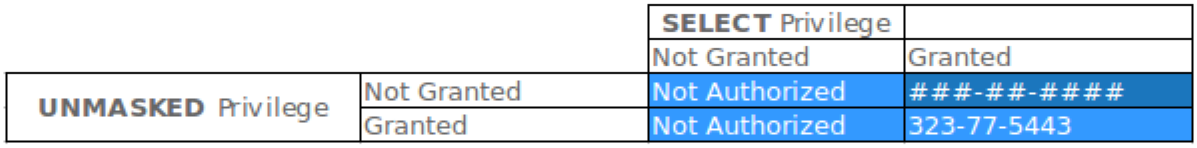
The mask expression could look something like the following:

```
CREATE FUNCTION credit_mask(input varchar(19)) RETURNS output
VARCHAR(19) LANGUAGE SQLSCRIPT
AS temp VARCHAR(19);
BEGIN
    SELECT LEFT(input,4) || '-XXXX-XXXX-' || RIGHT(input,4) into temp
FROM SYS.DUMMY;
    output := temp;
END;
GRANT EXECUTE ON credit_mask TO data_owner;
```

By using object privileges, authorization and data masking can be combined, for example:

```
GRANT SELECT ON credit_view TO end_user;
REVOKE UNMASK TO end_user;[9]
```

[9] https://help.sap.com/viewer/b3ee5778bc2e4a089d3299b82ec762a7/2.0.01/en-US/8c7968b893104ac6838a06855d607a6b.html



		SELECT Privilege	
		Not Granted	Granted
UNMASKED Privilege	Not Granted	Not Authorized	###-##-####
	Granted	Not Authorized	323-77-5443

Figure 6: Example of Pseudonymization

Secure Communications

Any personal data in transit between systems should be secured by means of encrypted channels. This prohibits the data being caught and viewed by eavesdroppers along the way. SAP uses 'SAPCRYPTOLIB', containing functions required for encryption, for securing channels.

Secure communications between the different ABAP client-server systems within the SAP landscape is accomplished by using the SAP concept of secure network communication (SNC). The secure communication happens on the application level. The technology secures communications for SAP protocols 'RFC' and 'DIAG'. SNC provides three levels of security. From less to more secure, they are: authentication only, integrity and privacy protection. Be sure to enable SNC in the SAP system properties.

For securing web protocol communications, SAP uses transport layer security: SSL. This applies to SAP Web AS[10] and AS Java[11] systems. In HANA, SSL is used to secure communications between databases (and cold storage), hosts, as well as processes on an individual host. A public key infrastructure, or PKI, is created automatically during installation. For some channels, TLS/SSL will have to be explicitly enabled. After that, SAP hosts start communication based on certificates, which are stored in the earlier discussed PSE's. The SAP HANA Security Guide provides more information on the topic.

Review which means of secure communications apply to your SAP system and use the SAP documentation accordingly to implement them.

Backups and Logging

One item not particularly highlighted in the GDPR text, is the balance of creating regular system backups versus the retention of personal data. The necessity to create backups remains absolutely unquestioned in this era of increasing ransomware attacks. Backups, however, broaden the scope of GDPR if your systems contain personal data. Therefore, we repeat: limit the amount personal data, but do make backups in case of a loss or breach to recover data.

Another somewhat underexposed topic is that of logging. The amount of available SAP logs is vast. For instance, we have the system log, security audit log and business transaction log amongst others. The security audit log (SAL) contains important information on suspicious activity; who accessed which table and at what time? Enabling (and creating backups of) this and other logs is essential to successfully auditing your system for GDPR and recovering after a breach.

Be sure to review your backups and logging and determine who has access to this data.

[10] https://help.sap.com/saphelp_nw70/helpdata/en/e6/56f466e99a11d1a5b00000e835363f/frameset.htm

[11] https://help.sap.com/saphelp_nwpi711/helpdata/en/bc/2ee9a2d023d64eac961745ea2cb503/frameset.htm

Conclusion

The upcoming EU General Data Protection Regulation will require a significant amount of time, resources, brainpower and a few headaches along the way for organizations to get in line with. To help SAP customers, Onapsis wishes to accompany you on your journey to compliance. With the Onapsis Security Platform (OSP) we can take the weight of keeping your SAP infrastructure compliant off your shoulders.

In a single glance, OSP automatically audits your SAP implementation and will give you an overview of the GDPR compliance status. Similar to our already existing policies for SOX, ISO 27001:2013 and PCI-DSS, our GDPR policy will be used to scan your systems and show points requiring attention to achieve and keep GDPR compliance.

Apart from monitoring compliance status, when scanning with OSP, you will be notified of all newly discovered SAP vulnerabilities your systems are exposed to on a recurring basis. Being informed about these vulnerabilities, including their remediation, will help you proactively protect your implementation from cyberattacks. The Onapsis Research Labs are constantly working to keep your SAP environment ahead of EU law and, in turn, keeping your business-critical SAP systems secure.

onapsis

About Onapsis, Inc.

Onapsis provides the most comprehensive solutions for securing SAP and Oracle enterprise applications. As the leading experts in SAP and Oracle cybersecurity, Onapsis' enables security and audit teams to have visibility, confidence and control of advanced threats, cyber risks and compliance gaps affecting their enterprise applications.

Headquartered in Boston, Onapsis serves over 180 Global 2,000 customers, including 10 top retailers, 20 top energy firms and 20 top manufacturers. Onapsis' solutions are also the de-facto standard for leading consulting and audit firms such as Accenture, IBM, Deloitte, E&Y, KPMG and PwC.

Onapsis solutions include the Onapsis Security Platform, which is the most widely-used SAP-certified cybersecurity solution in the market. Unlike generic security products, Onapsis' context-aware solutions deliver both preventative vulnerability and compliance controls, as well as real-time detection and incident response capabilities to reduce risks affecting critical business processes and data. Through open interfaces, the platform can be integrated with leading SIEM, GRC and network security products, seamlessly incorporating enterprise applications into existing vulnerability, risk and incident response management programs.

These solutions are powered by the Onapsis Research Labs that continuously provide leading intelligence on security threats affecting SAP and Oracle enterprise applications. Experts at the Onapsis Research Labs were the first to lecture on SAP cyberattacks and have uncovered and helped fix hundreds of security vulnerabilities to-date affecting SAP Business Suite, SAP HANA, SAP Cloud and SAP Mobile applications, as well as Oracle JD Edwards and Oracle E-Business Suite platforms.

For more information, please visit:
http://www.onapsis.com
https://twitter.com/onapsis