Preparing for the General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) goes into effect in May 2018 and will introduce stricter requirements around data consent, data transparency, and the handling of personal data. It is imperative that all companies understand how the GDPR will impact their HCM systems, data and processes.

"However fast regulation moves, technology moves faster. Especially as far as data is concerned."

About GDPR

General Data Protection Regulation or GDPR is a newly harmonized data protection law that comes into effect on May 25th, 2018 throughout all EU member states and European Economic Area.

It replaces the Data Protection Directive 95/46/EC and was approved by the European parliament on 14th April 2016.

The **EU General Data Protection Regulation (GDPR)** is the most important change in data privacy regulation in 20 years

Who needs to watch out?

All organisations (irrespective of the organisations location) that collect and process personal data of individuals who are within the European Union need to comply with this new law.

What is covered?

Processing of Personal data by any means and in any structured form including those intended as a part of the filing system.

So, do I need to be compliant?

The answer is a simple 'YES'.

As mentioned earlier, all organisations that use personal data need to be compliant with this new law. Personal data in this case is any information relating to an identified or identifiable person. So even if it is the local watch repair shop that would need your name, address and phone number- they will need to make sure that everything according to GDPR is adhered to.

What should you be aware of?

What should I do to store personal data?

First, there should be a clearly defined purpose for storing/acquiring/using data. This purpose should also be lawful as defined under the GDPR terms. Data is deemed lawful only if one of the following applies:

- The individual has given consent to process his or her personal data for one or more specific purposes
- Processing of data is required to fulfil a contract to which the individual is a part of
- If the data controller is part of a legal obligation for which data processing is necessary.
- Processing of data is required to protect the vital interests of the individual or any other lawful person
- Processing is required for a task carried out in public interest
- Or if there is legitimate interest in processing data pursued by the data controller or third party.

So cold calling companies – watch out!

What about the data itself?

All personal data should be adequate for the purpose it is stored/acquired for. It should also be limited and relevant for the exact purpose it is meant to fulfil. Organisations must ensure that there are deliberate security measures built to ensure data safety and make sure that there is lawfulness, transparency and fairness in data processing. Data also needs to be time bound i.e., if required only for a specific period, organisations must ensure that the time is defined and ensure data is purged after this. Organisation must ensure that data stays accurate at any given point in time, and take specific measures to keep data up-to-date, safe and secure.

Anything else that I need to be aware of?

Yes, Accountability.

GDPR aims to increase accountability of those processing data. Although very similar to the existing data protection legislation, GDPR aims to increase the transparency of data processing and take a tougher stance in enforcement. If organisations are found to be non-compliant they could hefty fines of up to 20 million euros or 4% of the annual revenue – whichever is higher!

My organisation uses SuccessFactors for employee data, will I get tools to stay compliant?

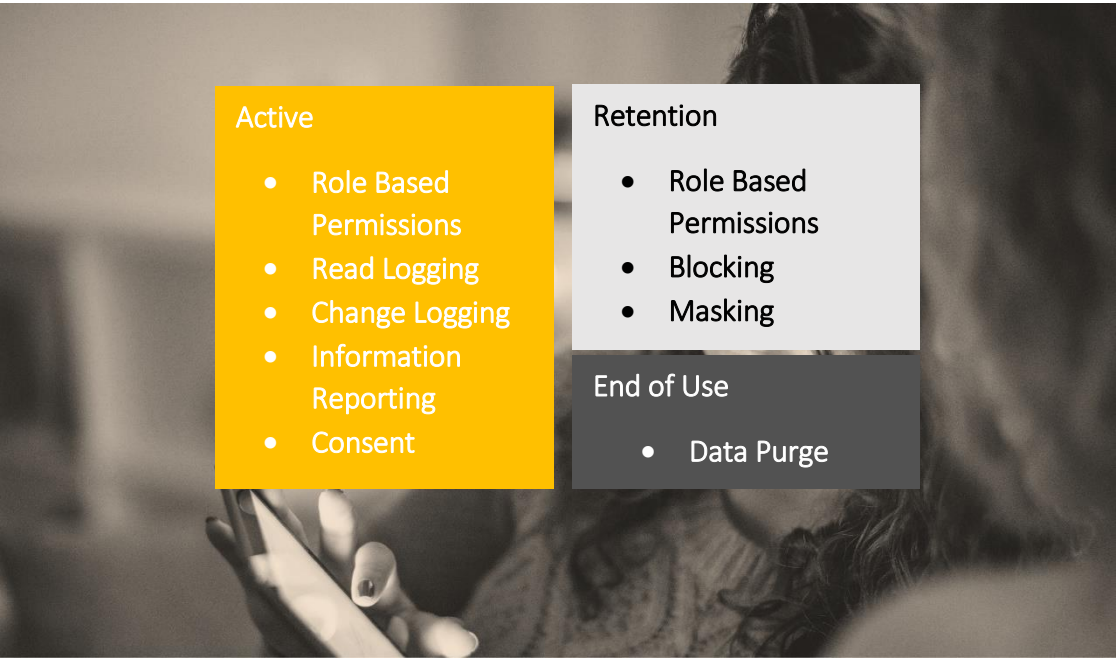
SuccessFactors and GDPR

With SAP's commitment for data protection, SuccessFactors has extended the existing products to stay compliant with the new legislation.

For ease of understanding, personal data has been classified into 3 phases during the employee life cycle

- **Active:** The phase during which data is processed for its specific purpose
- **Retention:** This is the phase after which data is not processed actively, but being held for specific purposes or for display purposes only
- **End of Use:** This is when data is no longer required in the system and can be purged.

During each phase, there are tools within SuccessFactors, helping you stay compliant:



Role Based Permissions

One of the best functionalities of SuccessFactors, Role Based Permissions or RBP's helps give access to data on 'Need to Know' basis. RBP's basically assign permissions based on a person's role within the company – example: HR of UK can only view data of UK employees. This is highly customisable and helps your organisation not only give the right access to employees, managers and admins, but also makes sure that no one has access to data that they should not have.

For this to work there are three elements:

- *Permission Groups:* Who gets access (example: HR of UK)
- *Permission Roles:* What access do they get (Example: View personal details)
- *Target Population:* On whom do they get this access (Example: Employees of UK)

In addition, SuccessFactors are updating RBP's to have the ability to define time periods for which historical records should be visible, including defining different intervals for different countries – which helps in Data **Blocking** required during the '**Retention Phase**'.

Read Logging

This new addition to existing audit reports, helps admins (who have the permission) to run a report to see who viewed sensitive data of any individual. Details of who viewed, when was it viewed are captured, regardless of the channel used (user interface, reporting or API calls).

Some fields within SuccessFactors are automatically classified as Sensitive, requiring no additional work from admins/partners. Example: Gender, Sexual Orientation, Ethnicity etc.

Change Logging

This new report, allows admins (with permissions) to run reports on all the personal data changes made for individuals. This report shows details of who made the changes, when was it made, for whom was it made and the current and previous values of data. Like Read Logging, this report captures details irrespective of the channel used to make changes (user interface, reporting or API calls).

Currently within the Employee Central module, you also can track Metadata Framework (MDF) changes.

Information Reporting

This helps to run a report to get all the personal details stored for any individual from within SuccessFactors. An example would be when an employee asks HR for all details stored against him/her. Admins only with the permission to run this report, can get the details. In addition, this report can also track when was it run and who ran it and for which individual was it run.

With the new legislation requiring data to be easily exported to be shared with individuals or competitors in a machine-readable format, the tools that already exist within SuccessFactors help you in staying compliant with this requirement. Reports can be downloaded/exported in .csv or .xls formats.

Consent

As a part of the legislation, you will need specific consent from individuals to process their data. SuccessFactors has extended the consent which was earlier available only within Recruitment to other modules as well. In some cases, the contract that is signed by the employee while joining the company can include statements about consent.

Masking

Data Masking helps to hide the data by default on the screen with asterisks (example: NI number display for an employee would be *********, unless the employee/HR admin explicitly clicks on the masked field to reveal the actual value). This helps prevent unnecessary exposure of personal or sensitive data on the screen.

Data Purge

Purging Data when not required is the best risk management strategy – and ensures you stay compliant with the new legislation as well. SuccessFactors helps you define data purging rules based on each country and each module - where you can specify for how long the record should have been active or inactive before it can be removed from the system completely. Example: You can specify in Germany, delete all performance records if it is older than 2 years for active employees, and 1 year for inactive employees.

Details of tools available within each module

Feature	Talent	EC	Payroll	Platform	Learning	ONB - Simplify	ONB-KMS	RCM	RMK	RP	Reporting	WFA	Enable Now	Mobile
1. Change Logging	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	✓	N/A
2. Read Access Logging	N/A	✓	✓	✓	N/A	✓	✓	✓	N/A	✓	✓	✓	N/A	N/A
3. Data Subject Info	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	✓	✓	N/A
4. Data Purge	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	N/A	N/A	✓	N/A
5. Data Blocking	N/A	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	✓	N/A	N/A	N/A
6. Consent	✓	N/A	N/A	N/A	N/A	✓	✓	✓	✓	✓	N/A	N/A	N/A	N/A

For More details on the Data Protection and Privacy Release, please click here.

Talk to us to understand and prepare for GDPR

+44 203 3719523
info@talenteam.com
www.talenteam.com

TalenTeam
Talent Solutions. Reimagined