sincron
HR SOFTWARE

THE IMPACT OF GDPR ON THE HR DEPARTMENT

FROM AWARENESS TO MEASURES TO ALIGN WITH THE NEW REQUIREMENTS

DISCLAIMER

This material is an interpretation of GDPR, as it is understood by the HR Sincron Company, from the date of publication. We studied the GDPR issue to align our own company to the new regulations and tried to understand its logic.

The principles are the same for all organisations, but the implementation and compliance with the GDPR will be tailored to the specific needs of each company, depending on each activity. We also feel that not all aspects and interpretations of GDPR are well-clarified.

Therefore, this eBook is only provided for informational purposes and should not be invoked as legal advice or to determine how the GDPR may apply to your organisation.

We encourage you to work with a legally qualified professional to discuss about the GDPR, how it specifically applies to your organisation and how to ensure the compliance with.

HR SINCRON SRL DOES NOT PROVIDE ANY EXPRESS, IMPLIED, OR STATUTORY GUARANTEE WITH REGARD TO THE INFORMATION IN THIS EBOOK.

This eBook is provided "as it is". The information and views expressed in this material may change without notice.

THE IMPACT OF GDPR ON THE HR DEPARTMENT

From awareness to measures to align with the new requirements

With the introduction of GDPR, the quote “with great power comes great responsibility” becomes extremely relevant to your HR department.

The data and their analysis have transformed the HR department into an important strategic partner within your company, now that you have at your disposal a wide range of tools to help you accomplish your tasks and achieve your objectives.

However, the access to sensitive and valuable information - such as personal data - brings a great deal of responsibility to managers and employees of the HR department: make sure that data is stored and operated safely and in accordance with the new regulations.

There has been much talk about GDPR lately and you have probably consumed a lot of information on this topic, but have you managed to clarify:

- ✓ *How does GDPR change the way you manage your personal data?*
- ✓ *How deep will be the impact on the HR department’s activity?*
- ✓ *What rights and obligations do you have to respect?*
- ✓ *What are the principles at the heart of GDPR?*
- ✓ *What measures and steps are required for alignment?*

INTRODUCTION

Through this eBook, we aim to help you find the answers to these questions and have a clear picture of the necessary activities to keep you in line with the GDPR requirements in due time.

WHAT IS GDPR?

GDPR is the most important change in data privacy legislation over the last 20 years and will change how your company and inherently your HR department can store and use personal information.

The **GDPR / General Data Protection Regulation** is part of the Data Protection Regulations in the European Union and will replace the current Data Protection Directive.

GDPR aims to standardise and reinforce the rights of the European citizens on data privacy. This means that any organisation that operates with people's personal data must meet new standards of **TRANSPARENCY**, **SECURITY** and **RESPONSIBILITY**.

To harmonize the legal framework in EU countries, the three major objectives of GDPR are:

1. Consolidating the rights of individuals;
2. Strengthening the obligations of the company;
3. Dramatic increase in sanctions in case of non-compliance with the law.

From the HR perspective, GDPR has the role of building a trust chain between the three actors involved:

- **Data Owner** - company's candidates and employees.
- **Data Controller** - your company as an employer.
- **Data Processor** - any company that is authorised by the data controller to process these business-critical data for your company.

Processing - any operation performed on personal data, whether or not by automatic means, such as collection, recording, organizational structure, storage, adaptation or modification, recovery, consultation, use, disclosure by transmission, dissemination or making available otherwise, alignment or combination, restriction, deletion or destruction.

To ensure the compliance with the GDPR, the whole process should start from the understanding of the rights consolidated by this new legal framework. We invite you to find them in the next section.

FAQ ABOUT GDPR

What is the role of GDPR?
GDPR has the role of protecting the privacy of people in the digital age. The new legislation has the role of harmonising data privacy laws among the EU countries.

Is GDPR relevant to me?
GDPR is relevant to your company if it processes the personal data of any citizen of the 28 EU Member States.

What data does GDPR target?
GDPR targets the processing by the company of any type of personal data, including those of the employees, candidates, and other people interacting with your company.

THE RIGHTS OF THE DATA OWNER

As an EU citizen, GDPR guarantees you the following rights:

The right to be informed - that is, to know everything that happens with your personal data, what it is used for, so you can access it, modify it and even revoke your consent.

The right to access personal data - you have the right to access your personal data whenever you want.

The right to be forgotten - You have the right to request the deletion of your personal data, except in certain cases, for example when personal data are used to comply with a legal obligation.

The right to restrict processing - you have the right to restrict processing e.g. when you think that personal data is not accurate and you have the right to request the verification of its accuracy.

The right to data portability - You have the right to move quickly and easily your data from one third party to another in absence of any other contractual conditions you need to be informed about before consenting to the processing of the data.

The right to rectification - You have the right to request the rectification of personal data if it is inaccurate or incomplete and especially when personal data has not been directly collected.

The right to object and restrict automatic decision-making - created to defend you against some negative potential decisions that could be taken without human intervention, such as automated data processing methods for evaluation purposes.

Your company processes the personal data of the employees from different departments (internal) and those of the candidates, clients, prospects (external).

An important part of these data is processed by the human resources department, which is why **the employees of the HR department in your company must know all the rights guaranteed by GDPR and you must make sure they are ready to respond, react and deal with the requests received.**

NEW RIGHTS FOR THE EMPLOYEES

As with any persons whose data is processed by the HR department, once with GDPR's entry into force, the employees of the company will also be entitled to more transparency about their personal data and the reasons why you need them.

→ The employee has the right to be informed about:

- ✓ *How long you are going to keep your data as an employer*
- ✓ *If you use the data to make automatic decisions*
- ✓ *If you intend to transfer your data abroad*
- ✓ *What data security warranties exist*

→ The employee must be informed about the **right to rectification** and his right to file a complaint to a supervising authority.

→ The employee has the "**right to be forgotten**", meaning he may ask you to delete your personal data under certain circumstances.

→ The HR department must ensure that any personal data of the employee is **accurate, complete and up-to-date.**

→ The employee must know **why certain data are collected** and be assured that they will not be used for other purposes without its consent.

Personal data = any information about an identified or identifiable individual.

Special data = more sensitive personal data, such as those revealing a person's racial or ethnic origin, or relating to health or sexual orientation; they are subject to stricter rules than "ordinary" personal data.

Identifiable individual = a person who can be identified, either directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more specific elements regarding its physical, physiological, genetic, psychological, economic, cultural or social identity.

Personal data protection = the right of an individual to have those characteristics that lead to its identification protected and the obligation for controllers and processors to take appropriate measures to ensure effective protection.

THE IMPACT OF THE GDPR REQUIREMENTS ON YOUR HR DEPARTMENT

The consequences at the level of the HR department will be major, but the GDPR requirements will help you build the trust between your company, as a data controller, candidates and employees as data owners, and third parties as data processors. Below are the GDPR principles that will impact the way you perform your daily activity.

THE NEED FOR AWARENESS
The GDPR has a direct effect on the data controlled by the HR department, so you have to make sure that each member of the HR team is up to date with the latest data privacy rules.

INVOLVING A DATA PROTECTION OFFICER
The Data Protection Officer (DPO) will estimate the impact of GDPR on your company's current processes and will intervene when not in line with the GDPR's requirements or other data protection laws. The sooner it is involved in the process, the more you will avoid costly mistakes.

ENSURING THE DATA OWNERS' RIGHTS
The people whose personal data is being processed will benefit from consolidating the rights under the GDPR legal framework, and your department will have to be prepared to respond appropriately to requests and in due time. Take into account the new rights, such as the right to data portability or the right to be forgotten, and think about how you can secure all these rights in day-to-day operations.

PROCESSING THE LISTS
According to GDPR, you are responsible for what happens to the data you control, so you must be able to demonstrate that your department and your company are acting in compliance with GDPR.

ENSURING THE SECURITY OF DATA PROCESSED BY THIRD PARTIES
You need additional security when HR data are processed by other organizations and you have to make sure that they also comply with the new regulations.

PRIVACY BY DESIGN
It is one of the core principles of GDPR for data controllers and refers to the compliance with the regulation from the very stage of product or service development - software applications used in HR should be designed and developed from the beginning in order to protect personal data.

PRIVACY BY DEFAULT
This principle refers to the fact that you have to take technical and organizational measures to make sure that you implicitly process only those personal data that are useful to you for a particular purpose.

AUTHORITY RESPONSIBLE FOR DATA PROTECTION
According to the GDPR, if you are operating in several EU Member States, you will have to cooperate with a single authority responsible for data protection.

CONSENT
If a person is not your company's employee, you need the free and unambiguous consent to process the data provided to you. Data can only be processed when it is consistent with the reason you collected it. You must also clearly define in the employment contract how the employee's data will be processed.

IS YOUR HR DEPARTMENT READY TO GREET THE GDPR?

Here are some questions you need to find answers to and which will help you identify the issues of your department and outline the action plan in order to comply with GDPR:

RECRUITMENT
Do you provide appropriate privacy notices to candidates, explaining how their personal data will be used? Are you sure that personal data collected at each stage of the recruitment process is required? Have you signed clear agreements with collaborative recruitment agencies?

BACKGROUND CHECK
Is it a necessary step and is it done only after the job offer has been made?

LEGAL GROUND FOR PROCESSING
Do you need a legal ground or other legal basis for processing the personal data? Is processing necessary to comply with law as an employer? Is your employees' monitoring legal?

PRIVACY NOTICES
Do you send clear and transparent privacy notices to your employees, explaining to them how their personal data is used and what are their rights as data subjects?

POLICIES AND PROCESSES
Have you reviewed your personal data management policies and processes?

PROTOCOL ON PRIVACY
Do you implement a data privacy protocol before starting any new process / project?

THIRD PARTIES IN THEIR QUALITY OF PROCESSORS
Have you reviewed the company's contracts with third parties to make sure they meet the GDPR requirements?

ACCESS REQUESTS OF DATA SUBJECTS
Do you have enough resources to cope with a possible increase in access requests from data subjects? Can you use the technology to simplify the process of identifying required data and to identify the information that can be disclosed?

MINIMISING DATA
Have you tried to minimise the amount of personal data you have and thus to reduce the amount of effort to respond to an access request received from the data subjects? Do you have a record keeping policy? Are the HR personnel and managers aware of the fact that records they keep can be disclosed?

STEPS FOR ALIGNMENT WITH THE GDPR REQUIREMENTS

After having responded to the questions in the previous section, you certainly have a clearer picture of your HR department status and you can begin to estimate the efforts that need to be made to comply with the GDPR requirements.

Even if you would like to end the process as quickly as possible, things do not work out as you snap your fingers, so you need a few steps to guide you to align the department with the GDPR requirements.

1. Form the team together with whom you can plan the strategy for compliance with the GDPR requirements.
2. Create a record of the information held - what personal data exists, where it is, why you need it, how and by whom it is processed.
3. Review the recruitment processes and documentation patterns of each stage of the recruitment process.
4. Review the privacy notices sent to the employees in order to ensure that they meet the new requirements.
5. Review the processes and systems to respect the rights of data owners and ensure the legal monitoring of the employees.
6. Implement data privacy policies and measures to align with the GDPR requirements.
7. Review the company's contracts with other recruitment agencies.
8. Review the agreements concluded with data processors, such as IT service providers or other outsourced services.
9. Review your data, policies and practices on data retention.
10. Set a program to notify the authority responsible for data protection about the violation of the regulation.

3 BASIC PRINCIPLES FOR PERSONAL DATA PROTECTION

SECURITY

According to the GDPR, any breach of security of personal data will have to be reported to the data protection responsible authority within 72 hours, unless the data is encrypted or do not identify individuals.

So you will need to review your current reporting mechanisms. The employees who may be affected by such a breach of personal data security will be notified immediately, "without undue delay".

It's important to consider any issues that might arise from how you store data at department level. Depending on the extent of the sensitive data you are processing, you may need a data protection officer to supervise the data processing activities within your organisation.

RESPONSIBILITY

GDPR introduces a number of new obligations for your company, which should make the transition from the compliance in theory with the regulation to concrete evidence demonstrating the alignment with the new requirements.

Once GDPR enters into force, organisations are expected to implement a series of measures, such as:

- *(Mandatory) appointment of a data protection agent;*
- *Making (mandatory) impact assessments on privacy;*
- *(Mandatory) consultations with data protection authorities prior to the beginning of data processing activities;*
- *Keeping records of all processing activities.*

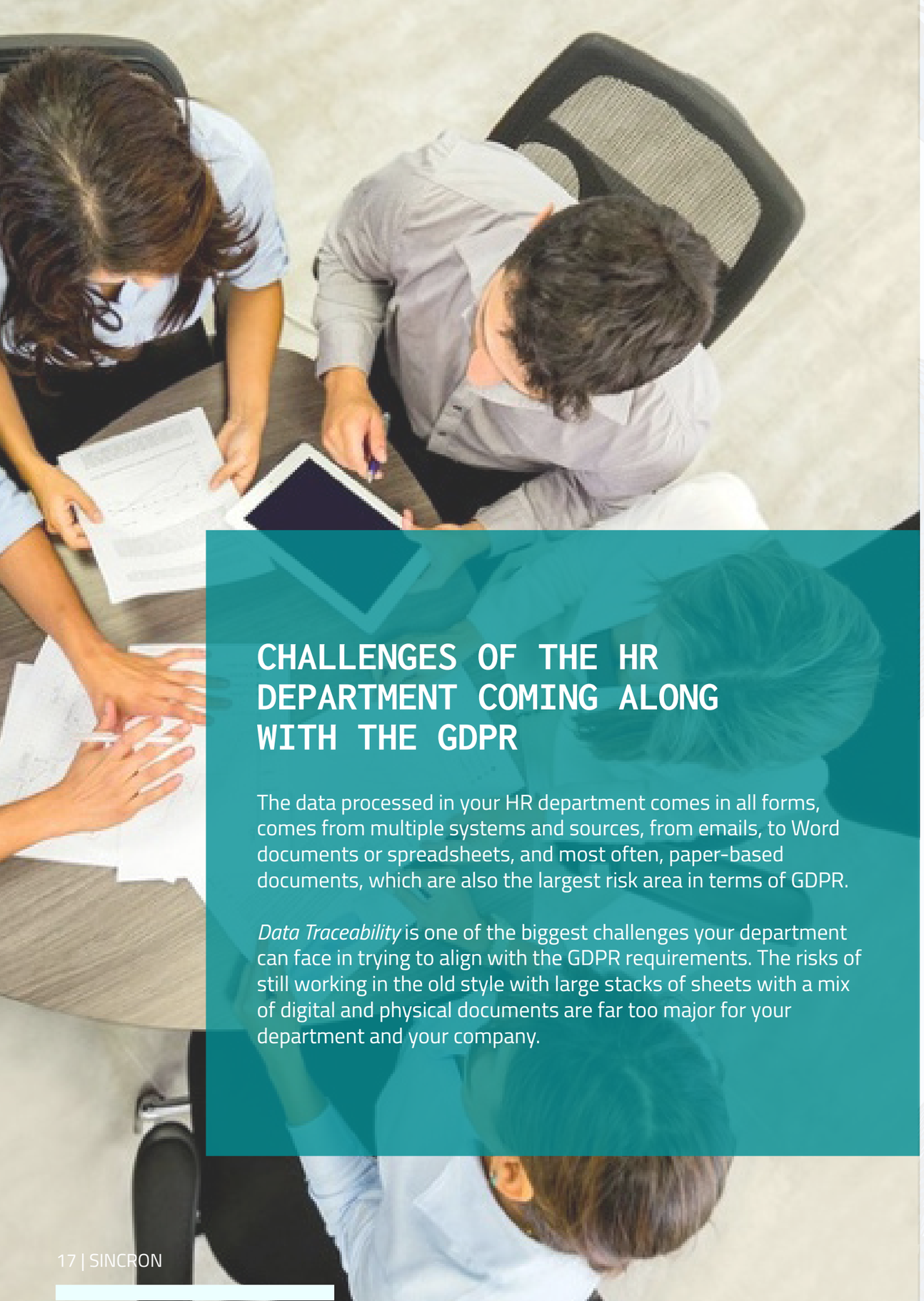
These new obligations will have a significant impact on how your company addresses projects that involve the processing of personal data.

TRANSPARENCY

The HR department, as a personal data operator, must be able to demonstrate that the data is processed in a transparent manner in relation to the data owner. These transparency obligations start when the data is collected and apply throughout their entire processing cycle.

The GDPR stipulates that information or communication to the data subjects must be concise, transparent, comprehensible and easily accessible and use clear language.

In other words, the information must not contain highly technical or specialised language or terminology. Furthermore, the information or communication must be provided to the data subjects in writing or by other means, such as by electronic or oral means, upon request. Finally, the information or communications must be provided free of charge, unconditionally.



CHALLENGES OF THE HR DEPARTMENT COMING ALONG WITH THE GDPR

The data processed in your HR department comes in all forms, comes from multiple systems and sources, from emails, to Word documents or spreadsheets, and most often, paper-based documents, which are also the largest risk area in terms of GDPR.

Data Traceability is one of the biggest challenges your department can face in trying to align with the GDPR requirements. The risks of still working in the old style with large stacks of sheets with a mix of digital and physical documents are far too major for your department and your company.

In order to overcome this challenge, besides aligning policies and processes, you will also need new tools to manage the personal data in a new manner - automated, centralised and secure. As such, implementing a suitable solution to manage all these HR data in a unitary system has become more imperative than just nice to have.

If you have already come to practical, operational questions such as:

- *Can I report to any interested person (employee, candidate) who has access to all personal data collected by the company about it and how does it process that data?*
- *Do I know exactly where I stored my personal data and can access, update or delete it when needed? Can I respect the right to be forgotten?*
- *Do I have the explicit consent of all the people whose data I own?*
- *How would I answer to a person who wants to know when and what kind of personal data I have collected or own about it? How fast can I respond - Can I observe the legal term of max. 30 days?*
- *Do I have permanent and easy access to all personal data I collect?*

....and the list could continue, you are probably at the point where you start to understand that the regulations could only be complied with by updating the set of tools that you use in HR.

Tidying and cleaning the "domestic kitchen" in advance is an absolutely necessary but not sufficient step. In order to be able to respect and implement the new standards of transparency, security and accountability, it is recommended to use a HR software.

When you want to sign or have already signed a contract with a HR software provider, consider that it becomes a data processor, so it must follow the same GDPR principles, such as applying since the stage of software concept the *"privacy by design"* and *"privacy by default"* principles.

HR software that is designed to meet the GDPR requirements will help you:

- *Automate the management of personal data;*
- *Have all the tools together so to be easy to control;*
- *Demonstrate that you have aligned with the GDPR requirements;*
- *Ensure data traceability and answer any question regarding the compliance with the rights and obligations regulated by GDPR;*
- *Respond in due time to the requests received from data owners regarding the processing of their data by your department.*

The policy outlined by your HR department for aligning with the GDPR requirements dictates how a HR software solution is tailored, and never vice versa.

Because each company and department has different needs, the software version you use should be personalised, tailored to your own requirements in order to be compliant.

CONCLUSIONS

We are preparing for GDPR - the most important change in data privacy legislation over the past 20 years, which changes how the HR department controls personal data.

With GDPR, your HR department has to meet new standards of TRANSPARENCY, SECURITY and RESPONSIBILITY.

Your department's efforts will have an important positive effect: by following the GDPR requirements, you will consolidate a chain of trust between you as a data controller, candidates and employees as data owners, and third parties as data processors.

The change involves the entire company, and HR employees need to know all rights guaranteed by GDPR. You will be assured that they are ready to respond, react and deal with the requests received. In addition, the employees of the company will also be entitled to more transparency about their personal data and the reasons why you need them.

Your HR department needs a clear strategy on the necessary measures to meet the GDPR requirements. Knowing the magnitude of the changes brought by GDPR, it's high time to identify potential departmental compliance issues, analyse the private data currently owned and review the approval procedures according to which the employees agree to keep their personal data.

Once the department policy is clearly defined, consider that:

- *Using HR software can relieve you of many headaches in order to be able to implement the GDPR principles from an operational point of view;*
- *The providers of IT solutions must apply the same principles to the products and services they offer.*

So we wish you much success in defining and implementing your own policy to align your HR department to the GDPR requirements!

ABOUT THE SINCRON HR SOFTWARE

Sincron HR Software is a People Management solution (HCM), managing in a centralised way the HR processes:

- *Organization management*
- *Recruitment*
- *Onboarding*
- *Personnel administration*
- *Time & attendance*
- *Payroll*
- *Performance appraisals and goals management*
- *Training management*
- *Internal communication and employee self-service*

One single platform means streamlining the processes, good speed of response, a high degree of control, an easy communication and the efficient use of resources.

As software and service provider for the B2B segment, the HR Sincron Company acts in most cases as a data processor, empowered by its clients, as personal data controllers.

In this respect, the HR Sincron Company is seriously treating the GDPR requirements, being in a full process of alignment with the provisions of the Regulation, so that on May 25th 2018 both the Sincron HR Software platform and all the related processes and activities are compliant with the requirements of the new legislation.

Thus, the Sincron HR Software clients use a software solution and additional services meeting the quality standards and complying with the new legal requirements.

DISCOVER SINCRON HR SOFTWARE

Now that you have understood the impact of GDPR requirements on your HR department's activity, we invite you to discover how an HR software may help you legally and safely manage the personal data of your applicants and employees.

ASK FOR A FREE DEMO