THE CONSEQUENCES OF THE RGPD IN THE PUBLICATION OF COLLECTIVE AGREEMENTS

Foreword

Since 1 September 2017, collective agreements must be made public and published in a national database accessible via the Internet at the following address

https://www.legifrance.gouv.fr/initRechAccordsEntreprise.do

The purpose of this national database is to facilitate access to the provisions contained in collective agreements and collective agreements and thereby strengthen the role of enterprise bargaining.

1) Agreements subject to this new publication obligation

The agreements and collective agreements concluded since September 1, 2017 must be made public and placed in a national database accessible from Légifrance. This obligation applies regardless of the level of the negotiation : company, establishment, inter-company, group or branch.

To note :

It is implemented article L2231-5-1 of the Labor Code which provides :

The branch, group, B2B, enterprise and establishment agreements and agreements are made public and entered into a national database, the content of which is published online in an easily reusable open standard.

After the conclusion of the agreement or agreement, the parties may agree that part of the agreement or agreement shall not be published as provided for in the first paragraph. This act, together with the full text of the agreement or agreement and the version of the agreement or agreement intended for publication, are attached to the deposit provided for in Article L. 2231-6. In the absence of such an act, if one of the signatory organizations so requests, the agreement or the agreement shall be published in an anonymous version, under the conditions laid down by decree of the Conseil d'Etat.

The conditions of application of this article are defined by decree in Council of State ».

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

By exception, since 1 April 2018, collective performance agreements, employee savings plans (profit-sharing, participation, company savings plans, B2B plans and Perco), as well as agreements determining the content of the ESP, are not more subject to the publication requirement.

However, this obligation applies to conventional collective termination agreements even though they include economic and social information about the company.

2) The possibility of publication in an anonymous version

Pursuant to Articles L 2231-5-1 and D 2231-7 of the Labor Code, the party in charge of filing an agreement or convention has the obligation to attach to it a publishable version of the agreement. or the collective agreement in an easily reusable computer format.

This version must be anonymous, that is to say, expurgated names and names of negotiators and signatory. The name of the company, its SIREN number, the name of the signatory trade union organizations and the quality of their representatives must, however, be included in the agreement or the agreement.

After receiving the deposit file, the Directe sends the publishable version of the text to the Directorate of Legal and Administrative Information (DILA) for publication on the Légifrance website (www.teleaccords.travail-emploi.gouv.fr).

3) The documents to be deposited

Whether it is a complete or partial publication, the person filing the agreement or agreement must attach the following documents to the filing :

- the full and signed version of the agreement ;

- its publishable version anonymized ;

- a copy of the letter, e-mail or receipt or an acknowledgment of receipt dated notification of the text to all representative unions at the end of the signing procedure.

In addition, in certain special cases, additional information and documents must be provided :

- when the company has separate locations, the text submitted is accompanied by a list of these establishments and their respective addresses ;

- when the parties decide that certain parts of the agreement are not to be published, they must attach a partial publication ;

- concerning the agreements submitted to referendum, the minutes of the result of the consultation must be annexed ;

- the filing of additional documents is also necessary in specific cases (example: agreement on actual wages).

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

These documents are preferably filed in PDF format, with the exception of the publishable version of the agreement, which must be in docx format (www.teleaccords.travail-emploi.gouv.fr).

To note :

The list of documents that must accompany the filing of the agreement or the collective agreement is set out in Article D 2231-7 of the Labor Code.

4) Possibilities of partial publication

Article L 2231-5-1 of the Labor Code allows the signatories of a group, inter-company, enterprise or establishment agreement to decide, once the agreement has been concluded, not to publish certain parts of it.

However, this decision of partial publication must be formalized by a reasoned and signed act :

- employees side : by the majority in number of signatory trade union organizations

- on the employer's side : by the legal representative of the group, the enterprise or the establishment for the agreements concluded at these levels and by the legal representatives of the companies concerned for business-to-business agreements (Article R 2231 is applied) - 1-1 of the Labor Code).

The partial publication act, the publishable version of the text and the signed full version are attached to the filing.

The collective agreement or agreement will be published with the indication that the publication is partial.

To note :

Since April 1, 2018, sectoral, professional or interprofessional agreements can no longer benefit from this option; they must be published in their entirety.

5) Questions still pending

Questions remain, however, about the nature of the act of publication.

Since the partial publication act is not a collective agreement, its negotiation would not be subject to the common law of collective bargaining and would only concern the trade union organizations signatory to the agreement (in this sense RJS 11/18 783 Jeansen and Thuleau, "The publicity of collective agreements, between transparency and secrecy").

Finally, neither the law nor the regulatory provisions specify the modalities of adoption of the partial publication act in the case of an agreement concluded with staff representatives not mandated by trade union organizations or ratified by 2/3 of the staff on the basis of a proposal from the employer.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

Such an act does not seem conceivable for these agreements with regard to the modalities of signature provided for by the texts.

However, no text of law for the time has come to settle these questions and to provide answers to the questions that they arouse.

6) Protection of the interests of the company

By unilateral decision, the employer can hide the elements affecting the strategic interests of the company.

It uses the faculty offered by Article L 2231-5-1 of the Labor Code.

This option is particularly interesting for agreements whose adoption procedures do not allow the conclusion of a partial publication.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

GDPR: impacts on companies

Foreword

The General Data Protection Regulation 2016/679 of 27 April 2016 (GDPR), which entered into force on 25 May 2018, replaces the system of prior formalities provided for by the Data Protection Act, a system based on the responsibility of the actors who will have to demonstrate the conformity of their treatments to this regulation at any time.

1) The specificity of the regulation: a direct and immediate application since 25 May 2018 in all EU countries without requiring, contrary to a directive, transposition in the different Member States. Treatments already implemented on this date must be brought into compliance with its provisions.

The National Commission on Computing and Liberties (CNIL), on its website and in several practical guides, analyzes the impact of the entry into force of this text, especially for companies. Our case study will therefore resume the content of the indications given by the CNIL concerning the relationship between employees and their company.

To note :

The GDPR applies to multiple fields and does not provide for specific rules on labor law leaving it to Member States to define, on this point, the adaptations that they deem necessary. The draft law on personal data definitively adopted by Parliament on May 14, 2018 and amending the Data Protection Act (Law 78-17 of January 6, 1978) contains only few provisions specific to labor relations, except in the processing of certain data.

Our case study therefore aims to present the changes introduced by the RGPD in comparison with the previous legislation.

2) The passage from the notion of prior formalities (declaration, authorizations) contained in the old directive 95/46 / CE of October 24, 1995 to a logic of conformity, of which the actors are responsible, under the control and with the accompaniment of the CNIL via the new European regulation.

Processors must implement all technical and organizational measures necessary to respect the protection of personal data, from the design of the product or service and continuously, that is to say to be able to demonstrate the compliance of their treatments any time.

The consequence of this empowerment of the actors is the abolition of the prior declarative obligations.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

Indeed, before their introduction in the company, the CSE must be informed about automated personnel management processes and any changes to them (Article L 2312-38 of the Labor Code).

This abolition of reporting requirements is likely to cause difficulties in the event of litigation. The absence of a mandatory declaration to the CNIL allowed a sanctioned or dismissed employee to rely on the inadmissibility of the evidence of the alleged facts drawn from an undeclared control device. This is no longer the case.

3) The establishments concerned by the GDPR : any organization, whatever its size, country of establishment and activity, may be concerned.

Indeed, the RGPD applies to any organization (public or private), regardless of its size, country of operation or activity as long as it processes personal data on its behalf or not, and that:

- it is established in the territory of the European Union;
- its activity targets European residents directly.

Example: A company established in France, exporting all its products outside the European Union must respect the GDPR.

The RGPD also targets subcontractors who manage personal data on behalf of other organizations (eg companies).

Subcontractors are subject to specific obligations: protection of personal data and privacy from the design of their service or product, advice to their customers, keeping a record of processing activities carried out for the account of their customers. The subcontracting contract must include a specific clause on the protection of personal data.

4) The data concerned are so-called personal data ie any information allowing to identify directly (surname, first name, for example) or indirectly (customer number, telephone number, number of registration for the management of a parking, biometric data, etc.) a person.

A person can be identified from a single datum (eg social security number) or from the cross of a set of data (person living at such address, born such day, subscriber to such magazine and activist in such association).

To note :

The IP and Mac addresses are personal data (*Cass, 1st civ 3-11-2016 No. 15-22.595 FS-PB*).

The collection of certain data must give rise to particular vigilance, particularly those relating to the beneficiaries of the rights of employees to the extent that they can provide information on their sexual orientation.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

The notion of file covers any structured set of personal data accessible according to certain criteria, whether this set is centralized, decentralized or distributed functionally or geographically (eg files arranged alphabetically or chronologically).

A personal data processing is an operation, or set of operations, relating to personal data, whatever the process used (collection, recording, organization, preservation, adaptation, modification, extraction, consultation, use, communication by transmission, dissemination or any other form of provision, reconciliation).

To note :

A file containing only company contact information (for example, company "Company A" with its postal address, the telephone number of its standard and a generic contact email "compagnieA@email.fr") is not a processing of personal data.

Moreover, a personal data processing is not necessarily computerized: the paper files are also concerned and must also be protected.

A processing of personal data must have a purpose, a purpose. It is not possible to collect or process personal data just in case it might prove useful someday.

5) The people targeted by the GDPR

- The controller is the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of the processing and on which the obligations laid down by the regulation.

- The person concerned by a treatment is the person to whom the data subject of the treatment relate.

- The recipient of a treatment is any natural or legal person, public authority, service or any other body that receives personal data, whether or not it is from a third party, the latter 'from any person other than the data subject, the controller, the processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.

6) The principles put in place by the GDPR

The Regulation is based on the principles according to which personal data must be :

- treated in a lawful, fair and transparent manner with regard to the person concerned ;

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

- collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes ;
- adequate, relevant and limited to what is necessary in view of the purposes for which they are processed (minimization of data) ;
- accurate and kept up to date ;
- kept in a form permitting the identification of the persons concerned for a period not exceeding that necessary for the purposes for which they are processed ;
- processed to ensure appropriate security of personal data, including protection against unauthorized or unlawful processing and loss, destruction or accidental damage (integrity and confidentiality).

To note :
Concrete actions must be implemented to respect the principles put in place by the GDPR :
- appoint a pilot ;
- register the files ;
- identify the treatments at risk ;
- respect the rights of individuals ;
- secure the data ;
- ensure, in the event of subcontracting, that the service provider complies with the GDPR ;
- appoint a data protection officer.

7) The Data Protection Officer (DPO) is obligatory for public bodies and companies whose basic activity leads to regular and systematic monitoring of large-scale people, or large-scale processing of data called sensitive or related to criminal convictions and offenses.

However, even if the company is not formally obliged to designate a DPO, the CNIL recommends appointing a person with internal relays to ensure compliance with the European regulation.

He is responsible for data protection compliance within his organization and is primarily responsible for :

- inform and advise the controller or subcontractor and their employees ;
- monitor compliance with the regulation and national data protection law ;
- advise the company on carrying out impact studies on data protection and verify their implementation ;
- to cooperate with and be the point of contact of the supervisory authority.

The DPO can be appointed internally among the employees of the company or externally. It can also be shared between several organizations or within professional associations or federations.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

To note :
The concept of large-scale treatment is not defined by the RGPD, which is why the CNIL has given illustrations to this notion of "large-scale treatment": treatments managing the data of travelers using public transport or those data relating to their customers administered by banks, insurance companies, telephone operators or Internet service providers.

8) The census of data imposes the obligation to keep a register of the processing of personal data.

Although this concerns only companies with at least 250 employees, the CNIL recommends its implementation in a broader way.

The objective is to identify the main activities of the company that require the collection and processing of data (examples with regard to the management of human resources: recruitment, payroll management, training, social declarations mandatory, badges and access management, etc.).

For each activity, it is necessary to list :

- the controller ;
- the objective pursued ;
- the categories of data used (eg payroll: surname, first name, date of birth, salary, etc.) ;
- the people with access to the data (the recipient - example: recruitment department, IT department, management, providers, partners, hosts) ;
- the shelf life of this data (the length of time during which the data is useful from an operational point of view and the archive retention period).

The register is under the responsibility of the manager of the company.

According to the CNIL, it is not necessary to list in this register purely occasional processing such as files created for a specific event operation such as the inauguration of a shop.

9) The objective assigned to the controller is to be able to prove at any time that the treatments he manages comply with the regulations.

It is therefore important to be able to determine the relevance of the data collected by verifying different points :

- circumstances of data collection: was there consent from the data subjects ? If not, does the collection meet specific obligations (collection required for the contract, compliance with a legal obligation, for example the processing of data relating to employees to communicate to the social security or tax administration ...) ? ;
- the nature of the information provided to the persons being collected and treated: were they informed of the purpose of the treatment and their rights ? ;

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

- the nature of the data collected with regard to the purpose of the treatment: only the data strictly necessary for the treatment can be collected and processed ;

- Information that only authorized persons have access to the data they need and that data is not retained beyond what is necessary.

10) Specific cases of data processing involving increased vigilance

This refers to treatments whose purpose or effect is :

- The evaluation of personal aspects or the notation of a person ;
- Automated decision making ;
- Systematic monitoring of people: telemonitoring, monitoring of employees' social networks, analysis of the social networks pages of job candidates, attendance time management tools (eg badge), geolocation systems ;
- The processing of sensitive data. Are concerned data revealing the allegedly racial or ethnic origin, relating to political opinions, philosophical or religious, relating to trade union membership, health or sexual orientation, genetic or biometric data, offense data or criminal conviction ;
- Processing of data concerning vulnerable persons (for example : minors) ;
- Innovative uses or the application of new technologies (example: connected object) ;
- Exclusion of the benefit of a right, service or contract.

This refers to treatments whose purpose or effect is:

• The evaluation of personal aspects or the notation of a person;

• Automated decision making;

• Systematic monitoring of people: telemonitoring, monitoring of employees' social networks, analysis of the social networks pages of job candidates, attendance time management tools (eg badge), geolocation systems;

• The processing of sensitive data. Are concerned data revealing the allegedly racial or ethnic origin, relating to political opinions, philosophical or religious, relating to trade union membership, health or sexual orientation, genetic or biometric data, offense data or criminal conviction;

• Processing of data concerning vulnerable persons (eg minors);

• Innovative uses or the application of new technologies (example: connected object);

• Exclusion of the benefit of a right, service or contract.

When data processing meets at least 2 of these 9 criteria, a Privacy Impact Assesment (PIA) must be conducted. The CNIL has put in place software facilitating the conduct and formalization of impact analysis : https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

To note :

Article 8 of the draft law on the protection of personal data adopted by Parliament on 14 May 2018 prohibits the processing of sensitive data. Insofar as the purpose of the processing requires it for certain categories of data, this prohibition will not be subject to this prohibition, in particular the processing according to standard regulations established by the CNIL implemented by the employers and relating to strictly biometric data. necessary to control access to workplaces as well as devices and applications used in the context of the tasks entrusted to employees, trainees or service providers.

For the sake of simplicity and support, the CNIL will not require the immediate completion of an impact assessment for existing treatments that have regularly been the subject of a prior formality with the CNIL before May 25 2018 (receipt, declaration of conformity to certain standards, authorization, opinion of the CNIL), or which have been recorded in the register of a computer and freedom correspondent. The companies concerned have a period of 3 years from 25 May 2018 to carry out this impact study. This tolerance does not apply to processing prior to May 25, 2018, which has been regularly implemented but which has undergone a substantial change since the completion of their prior formality.

11) The special case of data transfer outside the EU

In this case, it will be necessary to check whether the country to which the data are transferred has data protection legislation and is duly recognized by the European Commission.

This is is available at the CNIL.

The company will have to legally supervise its transfers to ensure data protection abroad.

12) Employee information

<u>The data collection medium, whatever its nature (form, questionnaire, etc.) must include the information listed below :</u>

- the identity and contact details of the controller and, where appropriate, the representative of the controller ;
- where applicable, the contact details of the data protection officer ;
- the purposes of the processing for which the personal data are intended and the legal basis of the processing ;
- the categories of personal data concerned ;

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

- where appropriate, the recipients or categories of recipients of the personal data (company internal service, service provider, etc.) ;
- the shelf life of the data ;
- the conditions according to which the interested parties can exercise their rights (via their personal space on the website of the company, by a message on a dedicated email address, by a postal mail to an identified service ...) ;
- in the case of transfer of data outside the European Union, the indication of the country concerned, the existence or absence of an adequacy decision issued by the European Commission or the reference to appropriate or adapted safeguards and the ways to obtain a copy or the place where they were made available.

In addition, it is imperative that this information be transmitted :

- as soon as the data are collected if they are collected directly from the employee (for example when they are hired) ;
- up to one month after collection if data is collected indirectly from another source.

However, this information does not have to be provided if the employee already has it.

To note :

Regarding the relationship between the company and its employees, the CNIL recommends informing them whenever they are asked for information (examples: administrative data updates, training request, maintenance form). evaluation, etc.) or when setting up a monitoring system, according to procedures to be determined according to the organization of the company (memo, amendment to the employment contract, information on the Intranet, enclosed mail pay slip etc.).

13) Guarantee and reinforce employee rights over their data : right of access, rectification, opposition, erasure (right to be forgotten), right to portability and limitation of treatment .

The GDPR imposes to provide employees with the means to effectively exercise their rights via a contact form on a website, a telephone number or an e-mail address.

The right to be forgotten is the right for a person to obtain from the controller the erasure, as soon as possible, of personal data concerning him / her. The grounds justifying the exercise of this right are exhaustively listed in Article 17 of the RGPD. In general, the RGPD imposes to proceed to the deletion of the data as they are no longer useful with regard to the purposes for which they were collected. It is recommended beyond setting data-deletion deadlines, providing automatic removal mechanisms or alerts on the tools used for file retention. In particular with regard to recruitment, information on unsuccessful candidates should be deleted unless they agree to stay in the company's "pool" (retention period limited to 2 years).

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

The right to a limitation of treatment means the right of a person to request that the data controller may not use certain data collected.

The right to portability, which is a novelty introduced by the RGPD, is the right for a person to obtain or even reuse the data concerning him for his personal needs but it involves the meeting of 3 conditions :

- the personal data were provided by the person himself ;
- the data are processed automatically, on the basis of the consent of the person concerned or for the performance of a contract ;
- portability must not infringe the rights and freedoms of others.

14) The security of the data aims at the measures to take, computer or physical, and depends on the sensitivity of the data treated and the risks which weigh on the people in case of incident.

Different actions must be implemented: antivirus and software updates, regular change of passwords and use of complex passwords, or data encryption in certain situations.

The company that has been the victim of a data breach (personal data has been accidentally or illegally destroyed, lost, altered, disclosed or unauthorized access to data) must be reported to the CNIL in the 72 hours if this violation is likely to represent a risk for the rights and freedoms of the persons concerned. This notification is made online on the CNIL website.

The data subject (s) should also be notified that their data has been potentially endangered.

To note :

If it is not possible to identify precisely who might be impacted by security breaches, the public should be notified of what may be very serious in terms of image.

15) A framework and a reinforcement of the scale of the sanctions implying that the controllers and the subcontractors can be the object of important administrative sanctions in case of ignorance of the provisions of the regulation: warning, formal notice, injunction of stop processing, suspend data streams etc.

Administrative fines may be, depending on the category of the offense, between EUR 10 million and EUR 20 million or, in the case of a company, up to 2% up to 4% of the annual global turnover. , the highest amount being withheld.

The latter amount should be related to the fact that, for transnational processing, the sanction will be jointly adopted by all the regulatory authorities concerned, thus potentially for the territory of the whole European Union.

In this case, one and the same decision of sanction decided by several authorities of protection will be imposed on the company.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

16) The control exercised by the CNIL of compliance with the RGPD since May 25, 2018 23 consists in carrying out verifications on the premises of the organizations, online, on hearing and on documents. The procedures for triggering controls also remain the same: the decision to carry out a control will be based on the annual program of controls, complaints received by the CNIL, information contained in the media, or following a precedent control.

The main novelty lies in the fact that the controls carried out on international actors will be carried out in a context of very strong cooperation which will lead to a harmonized decision with European scope.

The fundamental principles of data protection remain largely unchanged (fairness of processing, relevance of data, retention period, data security, etc.). They will therefore continue to be rigorously verified by the CNIL.

On the other hand, with regard to new obligations or new rights resulting from the RGPD (right to portability, impact assessments, etc.), the controls that will be carried out will be primarily intended, as a first step, to support companies towards a good understanding and the operational implementation of the texts. In the presence of organizations in good faith, engaged in a compliance process and showing cooperation with the CNIL, these controls will not normally lead to, in the first months, sanctioning procedures on these points.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

GDPR: data protection also applies to trade unions

Foreword

The Social and Economic Committees (CSE) and employee unions are still waiting for the production of RGPD standards by the National Commission for Informatics and Liberties (CNIL). In the meantime, the CNIL remains flexible as regards compliance.

Before the application of the European General Regulation on the Protection of Personal Data (GDPR) in France, the Social and Economic Committee of a company or an establishment obtained an exemption from the declaration of personal data to the Commission National Institute of Computing and Liberties (CNIL). But since May 25, 2018 the entry into force of the RGPD, these provisions of the CNIL no longer have legal value.

Today, the protection of data conditioned by the RGPD also targets the CSE. Indeed, within the framework of its missions and attributions (in particular for the social and cultural actions), the CSE is brought to collect and to treat personal data, in particular the data of the employees relating to their family and personal life as well as their health: surname, first name, address, family situation, function, telephone number and e-mail address, health situation, social and cultural activities, etc. In addition, a certain amount of personal information relating to employees is transmitted to it in the context of mandatory consultations (remuneration, etc.).

The CSE must therefore comply with the GDPR regarding the processing of these data :

- Collect the consent of employees regarding the processing of their personal data ;
- Inform employees about their rights ;
- Implement appropriate technical and organizational measures to ensure and be able to demonstrate that the processing is carried out in accordance with ;
- Keep a treatment record ;
- Plan measures to ensure the confidentiality of the processed data ;
- Appoint a delegate for the protection of personal data within the CSE.

As a consequence, the ESC must define precise rules for all personal data collected and make them public to employees. The CSE must then protect all of its information. It must assure employees that they will not be accessible to unauthorized persons. The CSE also undertakes not to misuse these data. In other words, each of them has a purpose. The CSE does not have the right to exploit this data for other purposes. It must have been authorized by the person or persons in question.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

Progressive implementation of the register of treatment activities

Article 30 of the RGPD provides for the establishment of a register of processing activities. This register makes it possible to register the data processing and to have an overview of what the CSE does with the personal data. This is a document in which all the personal data will be recorded. As an example, the CNIL proposes a registry model **(Appendix 1).** The format of this document is free. It can be digitally designed or presented in a more handwritten form. This register is a tool for piloting and demonstrating the conformity of the CSE with the RGPD.

The register of data processing activities makes it possible to register the data processing and to have an overview of the personal data.

3 steps to develop the record of treatment activities :

- Appoint a delegate for the protection of treatments,
- Register and group data processing by activity,
- Complete each activity sheet detailing the data processing.

The role of the Data Protection Officer (DPO)

In order to update the register of personal data processing activities and to ensure compliance with the GDPR, the CSE may appoint a Data Protection Officer (DPO).

This measure is not mandatory but strongly recommended in companies managing a lot of personal data. The appointment of a DPO may be useful in the context of the CSE's information and advisory mission to the controller or the subcontractor.

Currently there is no additional delegation time for the data protection officer. It is to be feared that this new system will lead to a little more responsibility and workload for the elected representatives, especially the designated Delegate. This work is likely to take time, especially in the coming months, while for many elected officials, the transition to CSE is underway.

The consent of the employee

The RGPD poses as a condition to solicit the consent in employees for the collection of their information. Staff representatives must define how to obtain this agreement, whether it is a document written and signed by the employee, or even a checkbox when consulting the website. In any case, the means used must clearly indicate to the data subject that he accepts the processing of his data.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057

Thus, employees are able to demand from the CSE :

- access to information concerning them;
- the rectification of their personal data;
- The deletion of their profile if necessary.

For this, the CSE must clearly explain to the employees the procedure (s) to follow. It is on this condition that regulation will be best observed.

The ESC has the obligation to put in place internal regulations that determine its operating procedures, its rules and those of its relations with the employees for the exercise of its missions. In order to be in compliance, a large number of EC / ESCs include a specific clause for data protection in the rules of procedure.

The information-consultation of the CSE in the application of the RGPD

Employers and human resources departments must also comply with the treatment of employees' personal data. As such, the elected CSE can be solicited in the compliance of the company. This can be done in particular via the CSE information-consultation (when performing an impact analysis of a particular treatment in particular) and / or the signing of a company agreement, in particular with the shop stewards.

Examples of possible involvement of unions and staff representatives :

- Computer Charter (and control of the use of computer equipment by employees);
- Internal regulations (control of access to premises, video surveillance, geolocation, telephone use, control of working hours, use of badges, code of conduct, etc.);
- Agreement on the transmission of personal data between the company and the CSE.

These practices are not mandatory but are recommended to allow the company a gradual compliance, without internal conflict.

The project is co-funded by the DG Employment of the European Commission. Agreement no. VS/2019/0057