Changes caused by the General Data Protection Regulation (GDPR)

NEWCHALLENGES

Séminaire OBES à Paris, le 13 septembre 2019

Avec le soutien financier de la Commission européenne

European Commission

CFE-CGC AGRO

The specific case of data transfer outside the EU

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

- A map of the world presenting data protection legislation is available on the CNIL website.

- Otherwise, the company must legally supervise its transfers to ensure data protection abroad.

A challenge: ensuring respect for new rights for employees: right of access, rectification, opposition, erasure (right of oblivion), right to portability and to limitation of processing.

- The GDPR requires that employees are provided with the means to effectively exercise their rights via a contact form on a website, a telephone number or even an e-mail address.

- The right to oblivion 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 GDPR. In general, the GDPR requires the deletion of data as soon as they are no longer useful with regard to the purposes for which they were collected. It is recommended that, beyond fixing data deletion times depending on the files, provide automatic deletion mechanisms or alerts on the tools used for file preservation. With regard more particularly to recruitment, information on unsuccessful applicants must be deleted unless they agree to remain in the company's "breeding ground" (conservation period limited to 2 years).

- The right to limit processing means the ability for a person to request that the controller cannot use certain data collected.

- The right to portability which is a novelty introduced by the GDPR constitutes the right for a person to obtain, or even to reuse, the data concerning him/her for his personal needs but it implies the meeting of 3 conditions:

- the personal data were provided by the person him/herself;

- the data are processed automatically, on the basis of the consent of the interested party or for the performance of a contract;

- portability must not infringe the rights and freedoms of third parties.

The new data security challenge

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

- The company victim of a data breach (personal data has been, accidentally or unlawfully, destroyed, lost, altered, disclosed or it has been found unauthorized access to data) must report it to the Cnil in 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.

- You must also notify the person (s) concerned that their data has been potentially endangered.

- Note: If it is not possible to identify precisely the people likely to be affected by the security breaches, you must notify the public which can be very serious in terms of image.

A reinforced and supervised scale of sanctions

- Data controllers and processors may be subject to significant administrative sanctions in the event of failure to comply with the provisions of the regulations: warning, formal notice, injunction to stop processing, suspension of data flows, etc.

- Administrative fines can amount, depending on the category of the offense, to 10 or 20 million euros, or, in the case of a business, to 2% up to 4% of annual global turnover , whichever is greater.

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

- In this case, a single sanction decision decided by several protection authorities will be imposed on the company.

Reinforced controls by the CNIL

- The CNIL must now carry out verifications on the premises of the organizations, online, on audition and on documents.

- The decision to carry out an inspection will be made on the basis of the annual programme of inspections, complaints received by the CNIL, information appearing in the media, or to follow up on a previous inspection.

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

- The fundamental principles of data protection remain essentially unchanged (fairness of processing, relevance of the data, retention period, data security, etc.). They will therefore continue to be subject to rigorous verifications by the CNIL.

- On the other hand, with regard to the new obligations or new rights resulting from the GDPR (right to portability, impact analyses, etc.), the checks carried out will essentially aim, firstly, to support companies towards a good understanding and implementation Reinforced controls by the CNIL in operational implementation of the texts. In the presence of bodies in good faith, engaged in a compliance process and demonstrating cooperation with the CNIL, these checks will not normally be intended to lead, in the first months, to sanction procedures on these points.

The consequences of the GDPR on Trade Unions and CSEs

The Social and Economic Committees (CSE) and employee unions are still awaiting the production of GDPR standards by the National Commission for Data Protection (CNIL). In the meantime, the CNIL remains flexible as regards compliance.

Context and evolution (1/2)

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

- Today, data protection subject to the GDPR also targets the CSE. Indeed, within the framework of its missions and attributions (in particular for social and cultural actions), the CSE is required to collect and process personal data, in particular the data of employees relating to their family and personal life as well as their health: surname, first name, address, family situation, position, telephone and email address, health situation, social and cultural activities, etc. In addition, a certain number of personal information relating to the employees is transmitted to it within the framework of compulsory consultations (remuneration, etc.).

Context and evolution (2/2)

- <u>The CSE must therefore be in compliance with the GDPR with regard to the processing of this data:</u>

Obtain 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;

Maintain a treatment register;

Plan measures to ensure the confidentiality of the data processed;

Designate a personal data protection officer within the CSE.

- Consequently, the CSE must define precise rules for all the 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 this data. In other words, each of them has a purpose. The CSE does not have the right to use this data for other purposes. It must have been authorized by the person or persons in question

Implementing progressively the registry of processing activities

- Article 30 of the GDPR provides for the establishment of a register of processing activities. This register makes it possible to identify data processing and to have an overview of what the CSE does with personal data. It is a document in which all personal data will be recorded. The CNIL offers, as an example, a model register (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 monitoring and demonstrating the CSE's compliance with the GDPR.

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

- 3 steps to develop the treatment activity register:

1. Designate a data protection officer,
2. Identify and group data processing by activity,
3. Fill in each activity sheet detailing the data processing.

The role of DPO

- In order to update the register of personal data processing activities and ensure compliance with the GDPR, the CSE may appoint a data protection officer (DPO). This measure is not compulsory but highly recommended in companies managing a lot of personal data. The designation of a DPO may prove useful in the context of the information and advice given by the CSE to the controller or processor.

- Currently, no additional delegation time is foreseen for the data protection officer. It is to be feared that this new system will lead to a little more responsibility and workload for elected officials, 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 employee's consent

- The GDPR sets the condition of seeking consent from employees for the collection of their information. Staff representatives must define the way to obtain this agreement, whether it will be a written and signed document by the employee, or even a check box when consulting the website. In all cases, the means used must clearly indicate to the data subject that he/she accepts the processing of his data.

Employees are therefore able to demand from the CSE:

- Access to information about them;
- The rectification of their personal data;
- The deletion of their profile if necessary.

- For this, the CSE must clearly explain to employees the procedure or procedures to follow. It is on this condition that the regulation will be best respected.

The CSE has the obligation to put in place internal regulations which determine its operating methods, its rules and those of its relations with employees for the exercise of its missions. In order to comply, many CE / CSE include a specific data protection clause in their internal regulations.

Information-consultation of the CSE in the application of the GDPR

- Employers and human resources departments must also comply with the processing of employees' personal data. As such, the elected members of the CSE may be asked to bring the company into compliance. This can in particular be done via CSE information-consultation (when carrying out an impact analysis of a particular treatment in particular) and / or the signing of a company agreement in particular with union representatives.

Examples of possibilities for union involvement and staff representatives:

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

These practices are not mandatory but are recommended in order to allow the company to gradually bring them into compliance, without internal conflict.

The consequences of the GDPR with regard to the publication of collective agreements

Since September 1, 2017, collective agreements must be made public and published in a national database, accessible by 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 conventions and thus strengthen the role of business negotiation.

Agreements subject to this new publicity obligation

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

- Note: Article L2231-5-1 of the Labour Code is applied.

- As an exception, since April 1, 2018, collective performance agreements, employee savings agreements (profit-sharing, participation, company savings plans, inter-company and Perco), as well as agreements determining the content of the PES are not any longer subject to the publication obligation.

- However, this obligation applies to collective agreement termination even when they include economic and social information on the company.

The possibility of publication in an anonymous version

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

- This version must be anonymized, that is to say the first and last names of the negotiators and signatories have to be erased. The company name, its SIREN number, the name of the signatory trade union organizations, the quality of their representatives must, however, appear in the agreement or convention.

- After receiving the filing dossier, the Direccte transmits the publishable version of the text to the Directorate of Legal and Administrative Information (DILA) for publication on the Légifrance site (www.teleaccords.travail-emploi.gouv.fr).

Documents to be filled

Whether it is a full or partial publication, the person depositing the agreement or convention must attach the following documents to the deposit:

- the full and signed version of the agreement;
- its publishable anonymized version;
- a copy of the letter, e-mail or receipt or a notice of receipt dated notification of the text to all representative unions at the end of the signing procedure.

In certain specific cases, additional information and documents must be provided:

- when the company has separate establishments, the text filed is accompanied by the list of these establishments and their respective addresses;
- when the parties decide that certain passages of the agreement should not be published, they must attach a partial publication act;
- concerning the agreements submitted to referendum, the minutes of the consultation results must be annexed;
- the filing of additional documents is also necessary in specific cases (example: agreement on actual wages).

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

Please note: The list of documents which must accompany the filing of the agreement or collective agreement is set out in article D 2231-7 of the Labour Code.

Partial publication

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

This partial publication decision must be formalized by a reasoned and signed act:

- on the employee side: by the majority in number of signatory union organizations

- employer side: by the legal representative of the group, the company or the establishment for agreements concluded at these levels and by the legal representatives of the companies concerned for inter-company agreements (article R 2231- applies 1-1 of the Labour Code).

- The partial publication act, the publishable version of the text as well as its signed complete version are attached to the deposit.

- The collective agreement or convention will be published with the indication that the publication is partial.
- Please note: Since April 1, 2018, branch, professional or interprofessional agreements can no longer benefit from this option; they must be published in full

Protection of corporate interests

- By means of a unilateral decision, the employer can conceal the elements prejudicial to the strategic interests of the company.
- He uses the faculty offered to him by article L 2231-5-1 d Labor Code.
- This option is particularly interesting for agreements the adoption procedures of which do not allow the conclusion of an act of partial publication.