White paper:

25 ideas received in digital employment law

Generally looking, the business world broadly welcomes the introduction of information and communication technologies (ICT), which allow us to improve productivity, review the working relationship, and which also encourage the emergence of new ways of organizing the work.

Through various issues (surveillance and control, methods of use by the employee, teleworking, collection and transfer of personal data, etc.), the ICT has managed to change the contractual balance between the employer and the employee and to break the temporal and spatial landmarks of the employment contract.

For this reason, the current legislation system is so focused on this particular question and, therefore, it has set up a regulation system to govern the rights of the employer and to protect the employee's freedom, under the supervision of both national and European courts, and of the National Commission for Information Technologies and Freedom (CNIL), the guarantor of the protection of personal data.

The content of this white paper may be subject to legislative, regulatory, or even jurisprudential amendments.

1. GDPR: The employer can refuse to act on a request of the employee to access the information referring to him/her

TRUE

The General Data Protection Regulation (GDPR) requires the employer to collect only those pieces of personal information that are relevant and about the objects pursued.

This implies that the employer defines reasons for processing of each data type and that he is able, at any time, to justify its legitimacy.

On the other hand, the employee does not only have the right to access the information referring to him/her, but he/she also has the right to correct a possible erroneous data and the right of opposition and erasure of the processing.

In this way, an employee has the right to access the information related to his/her recruitment, career history, assessment of professional skills (annual assessment interviews, ratings), to requests

for training and possible evaluations thereof, his/her disciplinary file, the use of his/her access control badge and the data from a geolocation device, and generally to any element used in making decisions about him/her (a promotion, a rise, a change in assignment, annual classification values, etc.)

However, the right to access has its limitations, and the employer can, under certain circumstances, refuse to give the requested data or documents:

if the right of access infringes the rights of third parties

For example, the employer can refuse to issue a copy of an email that implicates one of the employee's colleagues, or even to give the images from the video surveillance cameras where an employee is surrounded by third parties (for example, company clients).

If the right of access infringes the business secrecy or the intellectual property rights,

If the employee's request is obviously unfounded or abusive.

For example, an employee who continually requests data communication without any justification for it.

2. GDPR: The employer cannot limit the right to the erasure of personal data

FALSE

The right to the erasure of personal data was set up by the GDPR, and it allows the employee to request from his/her employer to erase all the collected data concerning him/her.

And yet this right is not unconditional, and it, in fact, concerns only those pieces of information that are no longer necessary concerning the purpose pursued by the processing.

Therefore, the right to erasure does not apply:

When data retention meets the legal obligation or in the case when the company is obliged to keep the documents for a specified period.

EXAMPLES:

The employee's Social security number is required to prepare a payroll, and therefore, it cannot be erased.

The pay slips must be kept for five years.

In general, most personnel management documents have a legal retention period with a particular purpose to enable the employer to respond to control of URSSAF (Organizations for the Collection of Social Security and Family Benefit Contributions) or to labor inspection.

Above and beyond this obligation, it is in employer's interest to keep this data as long as possible and he can use this motive to oppose an employee's request to erase his/her data.
when the implemented processing is of general interest,

when the processing is required as a part of a proceeding.

EXAMPLE:

The employee may refuse to grant a request for erasure if it deprives him of the elements needed for his defense in the context of a lawsuit against the employee.

3. GDPR: the employer cannot reveal the employee's personal details

TRUE and FALSE

In the hiring phase, only those involved in the recruitment process have the right to access personal information about the candidate.

Once the employment contract is concluded, the access to this information have only those in charge of human resources management, so as the representatives of relevant authorities such as health insurance funds, retirement funds, unions, etc.

The employee's supervisor may only have access to the information required for the performance of duties, such as evaluation data.

The staff representatives, for their part, have access to the information contained in the single staff register (name, date of entry, position, nationality, etc.), and the employer can transfer them other pieces of information only if the employee does not object to it.

EXAMPLE:

To present the number and age of the employee's children to the social and economic committee so the latter may suggest appropriate services and activities.

Therefore, the HR service must ensure the obtaining of such consent and that the employee does not object to the information transmission.

Of course, the employee should be informed about the context in which these pieces of information shall be transmitted, and it is forbidden to provide in advance a general authorization for data transmission.

Finally, under certain conditions, in case of a legal obligation or as a result of a court decision, the employer may be obliged to reveal the contact details of an employee.

EXAMPLE:

In this manner, the employer is obliged to disclose the employee's personal data to the Social security supervising physician, to a judicial police officer involved in a criminal investigation, to a bailiff with an enforceable title, etc.

Apart from these cases, any other communication of information about an employee is strictly forbidden if it has not been previously authorized by the latter.

4. The employer can read all the emails that come from the employee's business correspondence

FALSE

A distinction should be made between two sorts of email which may appear in the employee's business correspondence:

professional emails (related to the employee's job): they can be opened by the employer insofar as they are directly linked to the company,
personal emails (that are not in any way linked to the operation of the company): they are subject to the secrecy of correspondence and therefore cannot be opened by the employer (Supreme Court, from January 26, 2016, n° 14-15.360).

Emails from the employee's professional correspondence, whether sent or received, are presumed to have a professional nature and the employer has the right to open them in the employee's presence, unless the latter has identified them as personal (Supreme Court, from December 15, 2010, n° 08-42.486).

The messages are considered as « personal » if they are marked with a special mention like « personal » or « private ».

On the other hand, the mentions like « my documents », « confidential », « employee's family name » or employee's initials are not enough to give to these emails a status of personal messages.

The secrecy principle of personal correspondence applies even if the employer has prohibited the use of the company's software tools for personal purposes.

The protection of personal correspondence is no longer applied in case of an ongoing judicial investigation (for example when the employee is accused of stealing the employer's trade secrets) or if the employer has received a court decision authorizing him to access those messages.

To avoid any problem, it is in the HR service's interest to encourage the employees to mark their personal messages:

by marking their subject as « Personal » or « Private »,
by keeping them in a file named « Personal » or « Private ».

In all cases however, the employee must have previously informed his employees of the control of their professional messages, under the same conditions as for any other monitoring device.

Failing to do that, the device is unlawful and therefore it cannot be used to support a disciplinary sanction or to justify a dismissal of the employee.

Furthermore, the employer exposes himself to a risk to be penalized by the CNIL (in the percentage of turnover) and to face civil or criminal penalties for breach of privacy (up to 1 year of imprisonment and fine in the amount of 45 000 Euros).

5. The employer may request to receive an automatic copy of all messages received or sent by the employees

FALSE

The secrecy principle of private correspondence applies to the employee's professional correspondence, including the cases when the employer has forbidden its use for private purposes.

Requiring copies of all emails sent or received by the employees necessarily represents the breach of the right to privacy and correspondence.

It obviously represents an excessive monitoring procedure which is not justified.

6. The employer cannot install a keylogger device enabling him to remotely control all actions performed on a computer

TRUE

The keylogger software enables to record all the keystrokes that an employee performs on his/her computer.

It is an especially invasive control device allowed to be used only in extreme situations, for example if the employer justifies it with strong security imperative like suspicion of disclosure of company's trade secrets or act of unfair competition (CNIL statement, March 20, 2013).

Its use is punishable with 5-years imprisonment and with a fine of 300 000 euros; the same applies to the sale of certain data capture devices without the knowledge of the persons concerned (Penal Code, art. 226-3).

7. The employer may request from the employee to give his/her password

TRUE

To guarantee the respect of the employees' rights, and also to ensure certain traceability of actions on the company's computers, the CNIL recommends that each employee should have a sufficiently complex individual password which needs to be changed every 3 months.

Also, the CNIL considers that usernames and passwords (Windows session, messaging, etc.) are confidential and as such they cannot be given to the employer.

The passwords are personal and they allow the employer to find out what a given user has done on the company's network.

The fact of using someone else's password can be detrimental to the employee.

However, the courts consider that, in certain cases, the communication of a password by an employee to his/her employer is possible.

The employer may be aware of a password of an absent employee in the case when the latter keeps in his computer pieces of information that are necessary for the continuation of the company's activity and when he cannot access them by any other means.

The use of a password should not result in blocking the employer's access to any computer tool that he makes available to the employee.

The professional computer needs to be available to the employer, whether or not the employee is present in his/her workplace.

Moreover, the documents, files and messages that it contains are deemed as professional and therefore, the employer has legitimate access to them.

The Court of Cassation recognizes that the dismissal for serious misconduct of employees who deliberately refuse to give their password to the employee during their paid leave or medical leave, is justified when it reveals the intention to block the operation of the company (Supreme Court, May 23, 2012, n° 11-11.522, and February 19, 2014, no 12-27.611).

Therefore, an employee refusing to give his/her password is guilty insofar as he/she hinders the proper functioning of the company.

The use of the password should not submit the file access to the authorization of the employee nor to prohibit the employer's access to them.

However, special attention should be given to the fact that the use of an employee's password to access his/her computer does not allow the employer to consult and open the files which are marked as « personal » or « private ».

The latter remain protected by the secrecy principle of the private correspondence.

8. The employer cannot request from the employee to reply to emails outside of his/her working time

TRUE

The employee's working hours are strictly defined and regulated and the employer cannot ask from the employee to accomplish his/her professional duties outside of this working time.

In case when despite all, an employer requires from his employee to reply to professional emails outside of working hours, then the employee has the right to request payment for this period which is considered overtime work.

Thus, in the case when the employee has the proof of emails received outside of working hours in the form of a screenshot, he/she may obtain a salary reminder for these overtime hours, otherwise it may represent an offense of undeclared work.

In some cases, the situation is not so obvious, because sometimes the employee takes the initiative by sending the demands to the employer outside working hours.

To avoid any work overload, it is in the employer's interest to define and precise the terms of use of tools for business communication that he makes available to his employees.

The professional demands outside working hours related to NICT have multiplied and litigations are numerous, both in the domain of overtime work but also in the domain of stress and privacy intrusion.

The management necessarily requires the establishment of « truce » periods for professional correspondence (namely emails, but also vocal messaging, SMS, instant messaging, etc.) which correspond to the employee's minimum rest period.

This right to disconnection is also imposed by regulations since the companies of 50 employees and more are obliged to set up the means aiming to regulate the digital tools.

This issue is now part of the annual negotiation on occupational equality between men and women, and on the quality of life at work.

The purpose of these measures is to ensure the respect of time for rest and leave, and to keep the balance between professional life on one, and private and family life on the other side.

9. The employer may prohibit any personal use of the company's communication tools

FALSE

The CNIL believes that the employer cannot prohibit in a general and absolute manner the use of professional computer equipment for personal purposes.

The use of this equipment for personal purposes needs to be reasonable and, regarding the Internet connection, the ad hoc visits to websites on the workplace, only refer to those whose content is not contrary to the public order and good morals.

However, the European jurisprudence has reaffirmed the principle that « the employer's instructions cannot completely reduce the private social activities in the workplace» (ECHR, September 5, 2017, Req. 61496/08, Barbulescu/Romania, and February 22, 2018, Req. 588-13, Libert/France).

In this case, regulating does not imply prohibiting, and it is quite obvious that it is in the employer's interest to define use of these tools (whether in the rules of procedure or the IT charter) in a way that limits and reduces their use for private purposes.

However, he cannot lay down a general or absolute prohibition of the use of the equipment for purposes other than professional.

10. The employer cannot consult the employee's personal USB drive

FALSE

When an employee's USB drive is connected to a professional computer, the same presumption is applied as for the files and documents contained on the hard disc of that computer.
As long as the files and folders kept on the USB drive are not marked as personal, the employer may freely open them without the employee's presence (Supreme Court, February 12, 2013, n° 11-28.649).
The presumption of professional character is not applied when the drive is not connected to the

professional computer: the employer cannot demand it to be given just to see its content.

This is a violation of both privacy and the right to property (Supreme Court, July 5, 2017, n° 16-12.386).

11. The employee can give a private character to all the files, emails and documents contained in his/her professional computer

FALSE

Simple renaming of the business computer's hard drive to « personal data » is not enough to give a private nature to the files it contains, and to therefore benefit from the protection of personal documents (ECHR, February 22, 2018, n° 588/13).

The employee is not allowed to use for private purposes the entire hard disc of the professional computer made available to him/her by the employer, and which is supposed, above all, to contain the professional data.

On the other hand, the term « personal data » is a generic term and it can refer to professional files handled personally by the employee and not necessarily to the elements explicitly related to the private life.

In the same context, naming a folder or a file « My documents » or using an employee's name or initials is not enough to qualify its content as personal (Supreme Court, October 21, 2009, n° 07-43.877, December 8, 2009, n° 08-44.840, and May 10, 2012, n° 11-13.884).

12. The employer can only sanction those comments of the employee posted on social networks if the page is open to the public

TRUE

Defining whether the employee's comments made on the Internet or social networks are of a public or private nature gives rise to considerable dispute.

Traditionally, the case law commits to verify the configuration of the account to determine:

when the comments are on the page open to the public, they have a public character: therefore, the employer can sanction an employee whose comments are excessive or abusive,
when the comments, on the other hand, are posted on the page or a social network whose access is limited to a certain audience, their nature is therefore private and the employee cannot be punished for them.

In that manner, the abusive comments or insults made by a female employee about her director, but which are accessible only to those authorized by the interested party, in a very limited number, do not constitute public insults (Court of Cassation 1st civil chamber, April 10, 2013, n° 11-19.530). Also, when the comments are shared within a closed private group which can be accessed only by a very limited number of persons or members (for example 14 persons), such comments have private character and the employer cannot sanction them (Supreme Court, September 12, 2018, n° 16-11.690).

So, in order to attribute a private character to the comments made, except for the confidentiality configurations of the account, the jurisprudence also verifies if they were or were not shared with a limited number of persons.

Certain comments, however, even though they are made within a closed group accessible only to authorized persons, can be shared with tens or even hundreds of persons.

Therefore, it is likely that in case of litigation the judge would consider that they have lost their private character.

The jurisprudence systematically sanctions every intrusion by the employer into the employee's private domain.

The employer can be fined for the invasion of privacy when attempting to collect comments made on the employee's personal page with restricted access set up by the employee, for example when the employer uses a mobile phone of another employee of the company, who has the access to that network (Supreme Court, December 20, 2017, n° 16-19.609).

13. The employer can listen to all telephone calls made by the employee on his work phone

TRUE

The real-time listening or sound recording of phone calls made by the employee at their work can be carried out when necessary and they need to be proportionate to the objectives pursued.

In this context, the employer can install listening and/or recording device to:

educate his employees (for example, reuse the recordings as support to illustrate his point during the training),
evaluate them,
improve the quality of the service (for example, by studying the type of response provided to the client),
in some limited cases provided for by the law, to serve for the establishment of the contract or to complete a transaction.
However, there are some limitations regarding the device in question:

the employees, as well as the personnel representatives, need to be previously informed about it, like for any other monitoring device,
the employer cannot set up this device permanently (except in case of a legal obligation): he cannot record all the calls including when the aim is to combat the anti-social behavior,
the employer must use a device enabling the employee to turn off the listening or recording of personal calls,
the recordings need to be kept for up to 6 months,
access to information should be restricted to authorized persons.
The CNIL also advocates that the employee needs to have access to the reports of the recorded conversation so they could make observations to it.

14. The employer cannot link the listening of telephone conversations to a system for capturing the employee's work screen

TRUE

The linking of computer operations and phone conversations consists of registration of the image that appears on the screen of the employee's computer, simultaneously with the recording of the phone conversations.

However, the use of this device may lead to accidental capturing of some information and elements of private nature (personal emails, instant messaging conversations, etc.).

This is the reason why the CNIL forbids its use and considers that regardless of the objective pursued, a screenshot is likely to be neither relevant nor proportionate since it represents a fixed image of an isolated employee's action, that does not actually reflect his/her work.

On the contrary, it is allowed to link the recording of both phone calls and videos on the screen at the same time, under strict and precise conditions and only when it will be used for the sole purpose of training the personnel.

In this case it is imperative that the video recording is activated when the handset is lifted and it ends as soon as it is hung up.

15. Buffers are a lawful practice

TRUE

This activity is also recommended by the CNIL.

In this procedure, the employer or an authorized person listen to the recordings within days of their making and subsequently draft all necessary analytical documents.

After that the recordings are erased and the employer only keeps the analytical documents describing those recordings.

16. The employer cannot control the communications of the personnel representatives

TRUE

The employer cannot control the phone conversations of the personnel or union representatives: the latter need to have a phone line disconnected from any auto-switch because the employer has no right whatsoever to intercept the communications or to identify the correspondents of the personnel representatives (Supreme Court, April 4, 2012, n° 10-20.845).

Therefore, the employer cannot analyze the telephone records of the lines used by the personnel representatives.

However, the right to confidentiality is limited only to the telephone communications made by the employees protected within their legal mandate.

On the other hand, the employer has the right to completely control and intercept the communications made by the employee in carrying out his work and to identify its correspondents.

In practice, the protected employee shall have two phone lines: the first one used to carry out his work and which can be controlled by the employer, and the second one which shall be used exclusively to carry out the legal tasks entrusted to him/her, to which the confidentiality principle applies.

For the protected employee the introduction of this control system may represent a change in working conditions and therefore require his/her agreement.

EXAMPLE:

The use of a new software equipped with a dual listening system to check to quality of telephone calls of a protected employee working as a commercial adviser represents a change in working conditions and cannot be imposed by the employer (Supreme Court, December 13, 2017, n° 15-29.116).

17. The employer can compel the employee to show his/her badge to access the company's premises

TRUE

The employer can set up tools for individual control of access to the company's premises to secure the entrance to the building of facilities that are subject to restricted access.

These measures concern both employees and visitors.

The CNIL also approves the setting up of biometric devices.

The employer has also the right to set up the devices to manage employee's working hours and working time.

Unlike others, these devices cannot be biometric.

The employees, as well as the staff representatives, must be previously informed about it, like for any other monitoring device.

The system in place cannot be used to control movement within the premises (except in cases relating to safety: nuclear, chemical site, etc.).

It also should not impede the freedom of staff representatives to move while carrying out their professional tasks, nor to be used to monitor compliance with the time off for trade union duties.

The information is only accessible to the authorized members of services managing personnel, payroll or security.

The access data must be deleted 3 months after the registration and the data used for monitoring working time must be kept for 5 years.

18. The video surveillance cameras must not film the break area or resting space nor the employees at their workstations

TRUE

The video surveillance device must meet the specific objective of providing the security of both property and persons.

It cannot be used to control the facts and actions of employees.

The cameras can be placed at building entrance and exits, emergency exits and circulation routes.

They can also film those areas where the goods or valuable items are stored.

On the contrary, they cannot film the employees at their workstations, except in particular circumstances: for example, a bank employee who handles the money, warehouse containing valuable items where handlers work.

In this particular case, the camera should focus on filming the area to be secured rather than the employee himself).

Also, the cameras cannot be installed in break, resting and toilet areas.

It is also forbidden to film union premises or those reserved for staff representatives.

19. The video surveillance cameras may include microphones

FALSE

The video surveillance device must meet the specific objective of providing the security of both property and persons.

Their use must be proportionate to the intended purpose.

It is not therefore wise, besides filming, to plan a listening or sound recording of the premises.

This system is particularly intrusive for the employees and except in a specific case, it has no interest in the safety imperative pursued.

This is the reason why on several occasions the CNIL sanctioned the use of video surveillance systems which combined image and sound recording because it considered that the purpose pursued was in fact to monitor the employees and listen to their conversations.

EXAMPLE:

A company sets up a system of eight cameras, (each one includes a microphone to hear the sound and a speaker) filming eight employees, that is one camera per employee.

This system is obviously and without any doubt excessive because the company director puts his employees under constant and permanent surveillance and monitoring.

20. Only the company's security officer has access to video surveillance images

TRUE and FALSE

Only persons having the authorization of the employer, in the context of their duties, have the right to see the images registered as part of the video surveillance system.

Since this system has a purpose to ensure the security, the persons who are responsible for this domain within a company and who have access to the images recorded are security officer, guard, etc.

When the company does not have a specific security-related service, it is however allowed that the employer himself can have access to those images.

In any case, these persons need to be trained and made aware of how to implement this system.

21. The GPS device on a vehicle cannot be used to control the employee's working hours or the respect of speed limits

TRUE and FALSE

The control of an employee by using a geolocation system enables the employer to collect a certain number of data through the GPS.

The CNIL allows that this system can be installed for various purposes:

to facilitate the monitoring of services provided by the company,
to ensure the security of transported employees or goods,

comply with a legal or regulatory obligation (depending on the nature of the transported goods),
improve the organization of transport within the company (to optimize the technician routes for example),
to control the respect of the rules for use of the company vehicle made available to the employee (especially in the case when the employer forbids its use for private purposes).

Regarding the control of working hours, the CNIL allows that the geolocation can be used to track the employee's working time when it cannot be carried out by some other mean (EC, December 15, 2017, n° 403776, and Supreme Court, December 19, 2018, n° 17-14.631).

EXAMPLES:

A company controlling the duration of the response time of mobile technicians from their response declaration and has, when in doubt, the possibility to corroborate them by interviewing their clients to verify the time of arrival and departure of the employees, can place a system for geolocation only in case if it represents a more efficient mean of control.

Also, the mere fact that a self-reporting system and a mechanism for control of working time by a person in charge are not adapted for the intended purpose, is not enough to justify the use of the geolocation system.
However, in all cases, this system cannot be used for the employees who have freedom in the

organization of their work (for example, the employees with package agreement on annual working days), for which the employer does not have to control the working hours.

Finally, it is also forbidden to use the geolocations system to control compliance with the speed limits.

22. The employer can use the geolocation data to sanction the employee

TRUE

It is however important that the system has been implemented regularly.

Before the introduction of the geolocation system, the employer is obliged to individually inform the concerned employees and staff representatives about it.

The employees need to be familiar with the purpose of the processing, the categories of the localization data processed, duration of storage of this data, its recipients, the right of access and rectification as well as the right of objection, and their methods of exercise.

Moreover, an employer can use the geolocation system only for the purposes he previously presented to the employees. Otherwise, the system is not compliant and it can't be used.

If the information formalities have not been complied with or if the system does not comply with GDPR, the employer cannot take a disciplinary action based on the obtained geolocation data.

EXAMPLE:

A dismissal based on unlawfully collected geolocation data which are used by the employer to demonstrate the employee's presence in the workplace during Internet connection to pornographic sites is without real and serious cause.

In this particular case, the introduction of the geolocation system hadn't been discussed with the staff representatives, nor the employees had been individually informed before its introduction (Supreme Court, October 3, 2018, n° 16-23.968).

23. The employer may impose teleworking

FALSE

Teleworking is a type of work organization allowing an employee to regularly and voluntarily perform his/her professional duties outside the company's premises, thanks to information and communication technologies (ICT).

It can be set up within the framework of a collective agreement or, if none, within the charter drawn up by the employer after consultations with the Social and Economic Committee (SEC), if there is one.

It is, however, possible to set up a teleworking without the collective agreement or charger, using a simple agreement drawn up between the employer and the employee.
In other words, if you agree with your employee to telework, you can formalize this agreement and give it an official form by any means (employment contract, letter, email, etc.).

Whether at the time of hiring or during the execution of the employment contract, teleworking cannot be imposed on the employee.

To avoid any dispute, it is recommended to provide for teleworking in the employment contract (teleworking from the moment of hiring) or in an amendment (teleworking under contract).

There are, however, certain particular circumstances when the employer can temporarily introduce the teleworking without being obliged to obtain the employee's agreement, to ensure the continuity of the company's activity and guarantee the protection of the employees: epidemics, bad weather conditions, pollution peaks, floods, etc. But these situations are rather extreme and exceptional.

24. In the case of teleworking, the employee cannot set up a surveillance device in the employee's home

FALSE

In the process of implementing the teleworking, the employee may provide for the certain arrangement for time control and workload regulation, as well as the periods during which he can usually contact the teleworker (self-reporting systems (through computer-based scheduling system), computerized surveillance systems for calculating the connection time, etc.).

In case of setting up the system for employee's surveillance, it needs to be relevant and proportionate to the intended purpose, and the system to be used need to be previously discussed with the staff representatives and the employee need to be informed about it before its use.

Even in the case of teleworking, the control system needs to comply with the same requirements as if it had been implemented in the company's premises.

When the employee works from his/her home, the employer is responsible for providing, installing and maintaining all necessary equipment which would allow regular and normal work, except in cases when the employee uses his/her own equipment.

Under these conditions, access to the employee's private home may be necessary, but the employer must first request it in writing and the employee must give his/her consent.

In any case, since the employee's home represents an integral part of the intimacy of his/her private life, the implementation of an employer's request for access cannot in any way affect the employee's right to a normal private and family life.

25. The employer can have access to the employee's criminal record

TRUE and FALSE

A distinction must be made between the criminal record that mentions the possible criminal convictions of a person and the possible criminal record, opened in the case of an established offense, suspected offense, prosecution before the court or a judicial investigation.

There is no specific document providing for or forbidding the verification of employees' criminal records, and, therefore, the employer may request from a candidate during a job interview to

present the extract of his/ her criminal records, to check his/her criminal records and background.

However, the employer may not retain a copy of the document or allow such data to be specifically processed.

Also, the CNIL suggests that the mention of the criminal records verifications should feature in the personnel management file or indicate in the form « yes/no ».

Some so-called « sensitive » professions and businesses have a more stringent verification procedure of the employees' criminal records (form B2 or B3), which is carried out whether by the employer or by certain licensing authorities (for example, for security officers or maternal assistants).

These procedures can, thus, provide for the period during which the employer is obliged to keep the extract from the criminal record (3 months is usually used in these cases).

When there is no precise mention in the text, the document shouldn't be kept.

Concerning the criminal record, the analysis is somewhat different.

In the event of an offense, criminal prosecution or indictment, the employer may access the employee's criminal record only if the record mentions facts committed in the context of his/her work.

In such a case, the employer can then legitimately access to it for the following reasons:

either because he is the victim or a civil party (for example, in case of the embezzlement of the company's funds by an employee),
or because he is recognized as the co-author of the facts (for example in case of an accident involving a safety deficiency).