Teleworking: what are the good data security practices to adopt?

20 November 2020

On 29th October 2020, the French government hardened its position on the use of telework announcing that this practice far from being an "option“ in the current health crisis, was now "an obligation" and had to be implemented at 100% for those activities where it was compatible.

Included in the practical difficulties of implementing telework, is that of the very real challenge of protecting employees' personal data, and as a result, forcing companies to strengthen technical and organisational measures to guarantee the security of processes and exchanges.

Indeed, any remote organisation of work must necessarily be supervised and must include reinforced security measures in order to guarantee the security of the information systems and data processed remotely by the company's employees.

In order to support companies in the implementation of telework and in their efforts to secure personal data, the CNIL published a series of recommendations (recommandations) last April. **IT security and the adoption of good cyber security practices are essential for the use of teleworking by employers**.

It should be remembered that the implementation of teleworking, together with the necessary data security and information systems are the **responsibility of the company**, in its capacity as **data controller.**

The following is a check list of recommendations from the CNIL on the measures that must be taken in practice by companies to secure the data processed in telework, and to communicate the security instructions and recommendations to be given to employees:

WHICH SOLUTIONS SHOULD BE DEPLOYED BY COMPANIES?

Enact clear practices and instructions:

– An IT security charter should be communicated to employees incorporating the rules to be followed in the context of teleworking, detailing in particular the data protection rules and the penalties incurred in the event of non-compliance. It is also recommended that this charter be given binding force (e.g. by annexing it to the internal regulations). In certain circumstances, the employee's violation of the recommendations of this charter may justify disciplinary action up to and including dismissal (e.g. Court of Appeal, Limoges, Social Chamber, 4 February 2019 - n° 17/01419).

=> In this respect, has your company updated its IT charter on this point?

– Provide employees with a list of communication and collaborative work tools suitable for remote working, and which guarantee the confidentiality of exchanges and shared data.

➔ In particular, it is usual in teleworking to use discussion and video conferencing tools. As such, the CNIL published a communication on 9 April 2020 warning of the risks entailed when using these tools, notably when they do not offer sufficient guarantees of protection. In particular, the CNIL recommends:

- ✓ using only applications for which the publisher clearly indicates (indique clairement) how the processed data is reused (in the application itself or on its website, for example);
- ✓ reading users' comments on these applications;
- ✓ verifying that the publisher has put in place essential security measures such as encryption of end-to-end communications.

Reminder: the use of these communication and video-conferencing tools in the context of teleworking, as well as the security of the data processed via these tools, is the responsibility of the company in its capacity as data controller.

Grant Thornton
Société d'Avocats

Preparation of work-stations or posts

Employees should be equipped with workstations with a firewall, anti-virus and a tool to block access to malicious sites.

A VPN (Virtual Private Network) should be set up to avoid direct exposure of your services on the Internet.

WHAT RECOMMENDATIONS SHOULD BE MADE TO YOUR EMPLOYEES?

Use of equipment supplied and controlled by the company

It is recommended that their use be prioritised and as such to:

- raise employee awareness of the need to use the VPN provided by the company as much as possible;
- favour the exchange of data through the storage facilities available from the VPN rather than by e-mail;
- connect at least once a day to the company's VPN to apply any updates;
- Disable the VPN only when the employee uses services that use large amounts of bandwidth and that do not require the use of the corporate network, such as video streaming.

Pay particular attention if personal appliances and equipment are used!

If this is the case, the company must ensure that the following are implemented by their employees:

- ✓ the installation of an antivirus and a firewall ;
- ✓ the use of a personal account with limited rights, protected by a strong password and not shared with others;
- ✓ a regular updating of the operating system and the software used, in particular the web browser and its extensions;
- ✓ A regular backup of the work carried out and preferably on the company's own IT infrastructure.

In the same way, if employees use their personal mobile phones for professional reasons, the employer should:

- ✓ avoid the recording of any confidential information: secret codes, access codes, bank details, etc. ;
- ✓ activate the phone PIN code and set up an automatic phone locking time;
- ✓ activate an encryption of information on the employee's phone whenever possible;
- ✓ note the phone's IMEI number to block it in case of loss or theft;
- ✓ install software only from official platforms and avoid applications from unknown sources.

Securing and protecting your data: the company has a training role to play in regard to employees

The access and protection of your data requires the creation of a password that cannot be hacked:

If you think you have a strong password, take the CNIL test and check if you are in line with the expected standards of security: https://www.cnil.fr/fr/generer-un-mot-de-passe-solide.

Know how to identify phishing attempts: prevention and training

Employees should pay attention when they are in contact with:

- ✓ people they do not know, in particular if the issuer of a message invites the employee to click on links or open a file;
- ✓ a person known to them who sends an unusual communication. This information must be verified through another channel (telephone, SMS, e-mail);
- ✓ people who are actively creating a sense of urgency or risk. If necessary, any of the information communicated should always be checked by using another channel.

Ensure the security of communications.

Avoid transmitting confidential data via public storage services, online file sharing, collaborative editing or messaging services.

Favour the use of encrypted communication tools if the company does not provide secure communication tools and avoid free applications that offer little guarantee in terms of security.

Finally, it should be remembered that the ANSSI (National Agency for Information Systems Security) recommends the appointment of a contact person/referent for such a person is essential for the coordination of your company's IT security and to secure the use of teleworking.

WHAT ARE THE OTHER IMPERATIVES AN EMPLOYER SHOULD CONSIDER?

Although teleworking takes place outside the company premises, it can only be validly exercised in compliance with an employee's fundamental and individual freedoms such as the right to privacy or the confidentiality of correspondence. This reasoning also applies in the context of any data security related to telework.

As recalled by the Ministry of Labour in its Q&A session on telework, updated on 10 November 2020, no measures should be implemented that result in the constant and permanent monitoring of an employee's activity.

By way of illustration, the use of "keyloggers" which enable the remote recording of all actions carried out on a computer, are considered illegal by the CNIL, unless there are exceptional circumstances in regard to a strong but highly regulated security imperative.

WHO CAN THE EMPLOYER INVOLVE IN THE DATA PROTECTION PROCESS?

The implementation of measures and recommendations aimed at securing employees' personal data necessitates a certain horizontality to bring together the employer's different points of contact and reference within the company.

The employee representatives are as an example, one of the primary contacts in this context.

These very measures and the management of them will be more easily understood and accepted if validation is given by the representative bodies.

In this respect, any information coming from such representatives would both facilitate the measures being integrated into the data protection process and make the former and the employees aware of the stakes involved.

Furthermore, where the company has a Data Protection Officer (DPO) and bearing in mind the role staff representatives have to inform and advise both the former and the employees on data protection, the representative will necessarily have to collaborate with the employer on any measures to be taken in this area.

WHAT ARE THE MAIN SANCTIONS THAT AN EMPLOYER FACES IN THE EVENT OF A FAILURE TO ACT OR COMPLY?

As already mentioned, the employer as data controller, is bound by an obligation of security. This obligation is not to be considered as simply theoretical in the legislation.

Indeed, failure to take the necessary precautions regarding the security of employee information is punishable by a criminal penalty of five years' imprisonment and a fine of 300,000 euros.

In addition, an employer's failure to fulfil its obligations is punishable by sanctions imposed by the CNIL, which can range from a simple call to order, to an administrative fine.

***

Ensuring data security in the present context of widespread teleworking remains a major challenge for companies.

The lawyers of Grant Thornton Société d'Avocats specialised in social law and personal data law, as well as Grant Thornton's IT experts, remain fully mobilised and at your disposal to support and advise you in the implementation of all these actions.

Contacts

Caroline Luche-Rocchia
Attorney-at-law - Partner
E: CLuche-Rocchia@avocats-gt.com
T: +33 1 41 16 27 37

Alexis Grin
Partner – IT Risk Services
E: Alexis.Grin@fr.gt.com
T: +33 1 41 25 91 64

Nicolas Rémy-Neris
Attorney-at-law, Director
E : NRemyNeris@avocats-gt.com
T : +33 1 41 16 27 25

Pauline Garcia
Attorney-at-law
E : PGarcia@avocats-gt.com
T : +33 1 41 16 27 45

Islem Berkani
Attorney-at-law
E: IBerkani@avocats-gt.com
T: +33 1 41 16 27 40

Grant Thornton
Société d'Avocats

Grant Thornton Société d'Avocats
29, rue du Pont
92200 – Neuilly-sur-Seine, France
www.avocats-gt.com

About Grant Thornton Société d'Avocats

Grant Thornton Société d'Avocats supports its clients in all their strategic operations, whether in national or international context through multidisciplinary expertise in all areas of business law. The firm offers national and international customers all required services for the legal, tax and business management of companies. We deal in all business law matters: legal, tax, labour and contractual due diligences, mergers and acquisitions, tax law, VAT and international trade, global mobility, commercial law, employment law and finally business litigation