Recommendations to protect personal data in situations of mobility and telecommuting

The organisation, as data controller, may adopt the decision that certain activities within their company be executed in situations of mobility and telecommuting. Such a decision may be part of a management strategy, a general, or a partial strategy for certain areas or activities (for example, personnel who travels frequently) or it may be caused by exceptional or even force majeure situations.

If, in the first case, a prior planning must be carried out, in the second case, urgency situations may force the controller to put into place temporary solutions. When this occurs, it is compulsory, namely when the situation extends through time, to reflect about the situation and to perform an implementation of telecommuting in parallel. It must be taken into account that the State's resilience, the continuity of the business processes, and the rights and freedoms of data subjects whose data are being processed depend on it.

The organisation and the personnel that are involved in telecommuting actions must take the following recommendations into consideration.

RECOMMENDATIONS AIMED AT DATA CONTROLLERS

Below, a set of recommendations for the data controller is listed that the data controller will need to adapt to the specific situation of their business purposes:

1. Definition of an information protection policy for mobility situations

- Based on the data protection policy and the Information Security of the entity, and, as part of such entity, a **specific policy for mobility situations** needs to be defined that addresses the special needs and the particular risks introduced by the access to corporate resources from spaces that are not under the control of the organisation.
- In such policy, the determination must be made of what ways of remote access are allowed, what type of devices are valid for each way of access, and the level of access permitted pursuant to the mobility profiles defined. The responsibilities and obligations must likewise be defined to be undertaken by the persons hired.
- It is necessary to provide functional guidelines aimed at training the persons hired, as a result of such policies, and such guidelines must include at least the information described in the section “Recommendations addressed at personnel participating in processing operations” in this document.
- The personnel must likewise be informed of the main threats that may affect them when working outside the organisation as well as the possible consequences that may be materialised in case of breach of such directions, both for data subjects and for the employee.
- In such guidelines, a contact person must be identified to report any incident affecting personal data, as well as the suitable channels and formats to deliver such notification.
- The personnel must sign a telecommuting agreement that includes the undertakings acquired at the time to perform their tasks under a situation of mobility.

2. Election of solutions and service providers who are trustworthy and offer guarantees[1]

- The use must be avoided of telecommuting applications and solutions that do not offer guarantees and may give rise to the exposure of personal data of the personnel, the data subjects and the corporate services of the organisation, more precisely, through mailing and messaging services.
- Providers and data processors that offer verified solutions and sufficient guarantees must be approached that avoid, in the same sense, exposure of personal data of the personnel, the data subjects, and the corporate services of the organisation.
- If such persons were to access personal data, they shall be considered as data processors and the relation shall be governed by a contract or any other legal act that binds the processor with regard to the controller. This contract must establish the subject matter, the duration, the nature and the purpose of the processing, the type of personal data and the categories of the data subjects, as well as the obligations and the rights of the controller, pursuant to the terms established in Article 28.3 of GPDR.

3. Restriction of access to the information

- The profiles or the levels of access to resources and to the information must be set subject to the role performed by each person hired, in a way that is even more restrictive with regard to the profiles or the levels of access granted in accesses from the internal network.
- At the same time, additional access restrictions should be applied subject to the type of device from which the information is accessed (secured portable devices of the company, external personal equipment and mobile devices such as smartphones or tablets), and also depending on the location from which it is accessed.

4. Ongoing setting of the equipment and the devices used in the situations of mobility

- The remote access servers must be revised ensuring they are correctly updated and set in order to guarantee compliance with the information protection policy in mobility situations established by the organisation, as well as the control of the profiles of access defined.
- The corporate equipment used as clients must:
  - Be updated at the level of application and operating system
  - Have unnecessary services disabled
  - Have a configuration by default of minimum privileges established by the ICT services that may not be deactivated or modified by the employee
  - Only install applications authorised by the organisation
  - Have an updated antivirus software

[1] The report RBP/18 Security Recommendations in telecommuting situations and reinforcement of surveillance published by the CCN-CERT includes controls and specific security measures to be taken into account during the telecommuting situation, as well as a list of the companies operating in the cybersecurity area in our country who offer services and solutions within the context of remote access to corporate resources.

  - Have a local firewall activated
  - Have only the communications (Wi-Fi, Bluetooth, NFC, …) and ports (USB and others) needed to perform the endeavoured tasks activated.
  - Add encryption mechanisms of the information.

- If the use of personal devices of employees is allowed, because the fact of not incorporating the corporate equipment control to such personal devices entails a higher risk, apart from requesting the minimum requirements to be able to use them in the implementation of remote connections (for example, to have an operating system and an updated and original software), the possibility must be assessed of limiting the connection to a segregated network that solely provides limited access to resources identified as less critical and that are subject to a lesser level of risk.

5. Monitoring of accesses to the corporate network performed from the outside

- Monitoring systems must be established aimed at identifying abnormal behavioural patterns in the network traffic processed within the frame of a solution of remote access and mobility for the purposes of avoiding propagation of malware through the corporate network and the unauthorised use of, and access to resources.
- Security breaches affecting personal data must be notified to the Supervisory Authority and/or the data subjects, for the purposes of creating a resilient telecommuting background.
- The personnel must be informed, as part of the information protection policy for situations of mobility, on the existence and the scope of such control and supervision activities.
- If the monitoring activities were to be used as well to verify compliance with employment obligations of the personnel, the data controller must previously inform the employees in a clear, express and concise way and, as the case may be, to their representatives, with regard to the measures adopted within the frame of the control functions envisaged in the Employee’s Statute that must be performed within the legal frame thereof and within the limits inherent thereto.
- The monitoring mechanisms implemented within the context of remote access to corporate resources in situations of mobility or telecommuting must respect the digital rights established in LOPDGDD, more precisely, the right to privacy and the use of digital devices as well as the right to digital disconnection [2] in terms of labour.
- The setting defined in order to access the resources remotely must be reviewed on an ongoing basis to ensure it has not been altered or deactivated without a prior authorisation and it must likewise remain updated and adapted to an external risk background that is evolving continuously.

[2] Sections 87 and 88, respectively, of the LOPDGDD, https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

6. Rational management of data protection and security

- The measures and guarantees established in the policies defined that are to be established out of a risk assessment where the proportionality is analysed between the benefits to be obtained from a remote access and the prospect impact in case the access to personal information is compromised.
- The internal procedures must be envisaged in the policy to provide and to audit remote access devices, administration, and monitoring procedures with regard to the infrastructure, the services provided by processors and the way in which the policy is reviewed and updated with regard to the existing risks.
- The resources that may be accessed must be limited according to the risk assessment that the loss of the device and the exposition or unauthorised access to the information held entails.
- The remote access applications and solutions must be planned and assessed taking into account the privacy principles by design and by default throughout all the stages of deployment of the solution: since the definition of the requirements and the needs until the withdrawal thereof or of any of its components[3].

RECOMMENDATIONS ADDRESSED TO PERSONNEL INVOLVED IN PROCESSING OPERATIONS

The recommendations to the personnel must be included within the telecommuting policy of the controller and appear listed on the telecommuting agreement and adjusted to the specific situation of the tasks to be performed. A guidance on the content of such recommendations is as follows:

1. Respect the protection policy with regard to the information in situations of mobility defined by the controller

- The measures and recommendations included within the guidelines and the data protection and security of the information policy in situations of mobility defined by the organisation must be complied with, as well as the other implementing regulations and procedures thereof, namely with regard to the duty of confidentiality of the employee with regard to personal data they may access through their performing of their employment assignments.

2. Protection of the device used while in mobility and access thereto

- The employee may define and use robust access passwords that are different to those used to access personal email services, social media or any other applications used in their personal life.
- The employee must not download or install applications or software not previously authorised by the organisation.

[3] The document Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security published by the NIST includes an approximation based on the life cycle that envisages the recommendations and best practices to be taken into account during the starting, development, implementation, operation and maintenance phases as well as the withdrawal of a remote access solution and telecommuting.

- It is advisable for a connection of the devices to the corporate network in public places to be avoided, as well as the connection to open WIFI networks that are unsafe.
- The defined authentication mechanisms must be protected (Certificates, passwords, tokens, double factor systems...) to be validated before the remote access control systems of the organisation.
- If a corporate equipment is available, it must not be used for personal purposes, and access to social media, websites with advertising slogans and impacting advertising must be avoided, as well as all sites that may contain viruses or may encourage the execution of a damaging code.
- If the equipment that is being used to establish the remote connection is a personal equipment, the employee must avoid performing personal tasks at the same time as they perform professional tasks and they must define independent profiles to perform each type of task.
- The antivirus system installed in the equipment must be operating and updated.
- The legitimacy of the mails received must always be verified, and the employee must verify that the electric domain is valid and known, and they must not trust the download of attached files with unusual extensions or the establishment of connections through links included within the body of the mail that present a pattern that is outside normal parameters.
- If they may be managed by the person hired, it is advisable to deactivate WIFI Bluetooth and similar connections that are not being used.
- Upon completion of the working hours in a situation of mobility, the remote access session must be disconnected and access to the device must be switched off or blocked.

3. Guarantee of the protection of the information that is being handled

- Both in public places and in domestic environments, it is mandatory to take the necessary precautions to ensure the confidentiality of the information that is being handled.
- If paper is the usual format of the information, during situations of mobility it is important to minimise or to avoid the entry and the exit of documents in this format as well as to improve precautions in order to avoid unauthorised access thereto by third parties.
- The information that is on paper, including drafts, may not be discarded without ensuring it is adequately destroyed. If possible, avoid throwing full sheets or portions in hotel bins or public places or as part of the house waste that may be accessed by someone and, thus, personal information may be retrieved.
- More precautions need to be adopted to avoid unauthorised access to personal information, own information and third-party information, that is being handled, and no information form must be left in plain sight where the telecommuting is being performed and sessions must be blocked in devices where these are not being used.

- The content appearing on the screen must be hid from the looks of third parties. If work is usually performed at public places, it is advisable to use a privacy filter for the screen.
- To the extent possible, it is advisable to avoid being heard by third parties that are not a part to the conversation such as by using earphones or by moving to a space where the person hired is not accompanied.

4. **Preservation of the information at enabled spaces of the network**

- It is convenient to store the information generated during the situation of mobility locally in the device that is being used, and the use of shared storage resources or cloud storage resources provided by the organisation will be preferred.
- If the use is allowed of personal equipment, under no circumstance should applications that are not authorised by the entity’s policy be used in order to share information (cloud storage services, personal mailing, instant messaging, etc.)
- The corporate policy of security copy defined for each device must not be blocked or disabled.
- It is advisable to review and to erase on an ongoing basis residual information that may remain stored in the device, such as temporary files of the browser or documents downloaded.

5. **If there is a suspicion that the information may have been compromised, the security breach must be immediately notified.**

- Any anomaly that may affect the security of the information and the personal data processed must be notified to the controller as soon as possible, without undue delay, through the channels established to that end.
- In the event of an issue that may arise within the context of situations of mobility that may entail a risk for the protection of the information and the access to corporate resources, the employee must consult the Data Protection Officer and the security officer of the information or the profiles appointed for such purposes, and they must convey all relevant information to the extent known by the employee to such profiles.