Informative Note

On the recommendations and measures to be adopted to protect personal data in mobility situations and teleworking in the context of COVID-19

13th April 2020

AEPD recommendations to protect personal data in situations of mobility and telework

In line with our information note of 19 March on the security recommendations for teleworking made by the National Cryptology Centre and by the European Cybersecurity Agency, we consider it appropriate to summarise the security recommendations issued by the Spanish Data Protection Agency ("**SDPA**") in its technical note "Recommendations to protect personal data in situations of mobility and teleworking". The recommendations include the measures to be adopted by data controllers and their employees or collaborators for the processing of personal data.

Firstly, the SDPA points out that prior planning for teleworking is essential. However, in emergency situations such as the present one, it is possible to adopt provisional measures, without prejudice to the fact that, when the emergency situation is prolonged, it is necessary to adapt the implementation of measures for employee teleworking.

In this sense, the SDPA proposes a block of six recommendations aimed at those responsible for processing, which must be adapted to the economic activity they carry out, as follows:

- Define a specific information protection policy for remote work situations, which provides for the needs and risks in those cases where corporate information is accessed from spaces that are not under the control of the company.

- To use computerized solutions for remote work that offer enough guarantees.

- Limit access to information, creating access levels based on the tasks performed by the organization's employees, as well as restricting entry from certain devices or depending on the location from which access is gained.

- Periodically review the equipment, servers and other devices used for remote work, installing the relevant updates so that they are adapted to the company's teleworking policy. If employees use their own devices, it may be necessary to restrict their access only to information that is considered less critical.

- Monitoring of access to the corporate network from the outside, identifying abnormal behaviour in order to prevent the spread of malware and unauthorised use and access. In any case, this monitoring power must be made known to employees prior to its implementation, especially if it is used to verify compliance with their work obligations.

- Security breaches must be made known to the SDPA and to the interested parties, where appropriate.

- The measures adopted in the privacy and security policies must stem from the risk analysis carried out beforehand, which must weigh up the proportionality between the benefits obtained by remote work and the impact it may have.

- The teleworking policy must provide for internal procedures for the correct provision and auditing of the devices used for remote work.

The SDPA also proposes a series of measures aimed at employees or collaborators of the data controller who, in the performance of their duties, process personal data. Thus, the SDPA urges that these recommendations be included in the internal policies of the data controller, with special reference to the following aspects:

- Employees must respect the data protection policy implemented by the organization for remote work. Thus, it is up to the data controller to provide the guidelines and recommendations that they must comply with.

- Adequately protect the devices and accounts used to provide remote services. In this case, it is advisable to establish robust and different passwords for each account, as well as having different access codes for personal and professional accounts.

- Employees must take all relevant precautions to ensure the protection of the information they are dealing with, safeguarding confidentiality in all cases. Therefore, it is advisable to avoid the use of paper and to be careful when destroying it, as well as to close the session when the computer is left unattended to avoid intrusion by third parties.

- Save all the information generated in the corporate cloud available to the organization, avoiding storing it locally on the devices themselves.

- Immediately communicate any type of anomaly or security breach to the person responsible for processing or the Data Protection Officer that may affect the information and personal data processed.

In short, the SDPA establishes general recommendations aimed at guaranteeing the security of information and personal data processed in the context of teleworking. In view of the situation caused by COVID-19, which has forced many companies to adopt this working method in order to guarantee their economic continuity and adapt to a working model that they had not previously established or planned, it is appropriate to take this opportunity to redesign and complete internal information security and processing policies that include the digitalisation of work functions.

You can download the recommendations of the Spanish Data Protection Agency here.

We hope that the information will be useful and of interest to you. At Andersen Tax & Legal we have created a multidisciplinary team to deal with all the questions that may arise on this aspect or in relation to the COVID-19 and all the professionals of the firm are at your disposal.

For more information please contact:

Isabel Martínez | Director of Privacy, IT & Digital Business
isabel.martinez@andersentaxlegal.es