Should the controller reassess the relationship with its processor in the context of this new pandemic?

MPR PARTNERS
MARAVELA, POPESCU & ROMAN

*Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("**General Data Protection Regulation**"), controllers must only use processors that provide sufficient guarantees regarding their capability to implement appropriate technical and organizational measures to ensure that all processing activities are performed and protected in line with the legal requirements.*

In this respect, before engaging the services of a processor, the controller must perform a proper assessment of the processor's capabilities to process the entrusted personal data in a secure and confidential manner, in accordance with the provisions of the General Data Protection Regulation.

The duty of care that needs to be observed by the processor must be reflected into a contract concluded with the controller. Such contract must stipulate that the processor will take all technical and organizational measures to ensure a level of security in accordance with the risk, including inter alia as appropriate:

(i) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(ii) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(iii) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

2. Times are changing, should the processors be reassessed?

Due to the new severe acute respiratory syndrome coronavirus 2, known as SARS-CoV-2, emergency measures were taken throughout the world in order to contain the spread of and fight against the effects of SARS-CoV-2. One of those measures was for the companies, where possible, to send their employees to work from home.

Does this new scenario change the controller's initial assessment on the processor's ability to ensure the technical and organizational measures in relation with the processing of personal data?

The answer is yes, if the controller considered only the capabilities offered by the processor within its premises. It is possible that most controllers did not took into account the processor's readiness to ensure the secure processing of personal data via remote access by employees working from home. From a security perspective, any remote access to data might present a risk that needs to be properly addressed.

The EU Agency for Cybersecurity ("**ENISA**"), the National Cyber Security and Incident Response Teams ("CERTs") and the national Data Protection Authorities ("**DPAs**") are all advising on the need to maintain an adequate level of cybersecurity when working from home and recommend companies to take measures such as:

(i) to ensure that the corporate VPN solution scales and is able to sustain a large number of simultaneous connections;

(ii) to provide secure video conferencing for corporate clients;

(iii) all the corporate business applications must be accessible only via encrypted communication channels;

(iv) access to application portals should be safeguarded using multifactor authentication mechanisms.

These recommendations were issued not just because there is an increase in the number of people that are working and having access to systems remotely, but also because in this state of emergency the number of cyber-attacks, such as denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks, man-in-the-middle (MitM) attack, phishing and spear phishing attacks, drive-by attack, password attack, intensified. Both situations can result in an increase number of security incidents, from which a lot of such might prove be data breaches.

In this context, it is evident that, from a security perspective, we operate in a scenario, that is different than the one took into account by the controller when selecting the processor. The initial assessment of the risks presented by the data processing, such as accidental and unlawful destruction, loss, unauthorized disclosure of data, translated into security measures meant to mitigate the respective risks. But now the scenario is different, and the risks presented by the data processing in the new environment (working from home) might require different security measures in order to mitigate the such.

In this respect, the controllers should perform at least an assessment on the security measures in place and if such measures are enough to ensure that their processors are still fit to handle the entrusted personal data.

3. Conclusion

We live in a new era, where the risks are multiplying and endanger the security and integrity of data. It is important to pay attention to each and every change that might have an impact on the relationship the companies developed with their processors. This might be just one of the problems that might occur. Data protection should not be treated lightly in these times, because the consequences of the events occurring in relation with personal data can affect the companies on a long term.