The General Data Protection Law's Impacts on Remote Work

04.11.2021 3 min read

Authors

Felipe Palhares

Topics

Labor and Employment | Data Privacy and Cybersecurity | ANPD | GDPR | Home Office

The transition from in-person to remote work can present complications when it comes to protection of personal data, particularly when the transition is an abrupt one, such as many organizations experienced in the covid-19 pandemic.

Since September 18, 2021, when the General Data Protection Law (LGPD – Lei Geral de Proteção de Dados Pessoais) came into effect, all processing of personal data must comply with the requirements under the legislation. If concerns over personal data processing already existed with in-person work, remote work has raised them to another level.

Just to be clear, if your organization has implemented remote work, it is constantly processing personal data. Sending and receiving e-mails, exchanging messages on corporate communications apps, making video and audio conference calls, along with many, many other daily activities, involve collecting, sharing, processing and storing personal data.

In this scenario, two main issues merit attention. The first is ensuring that there is a legal basis for processing data. The LGPD only allows data to be processed if the data controller (the organization that determines the purposes and means for processing the data) identifies which of the cases provided for under article 7 and article 11 of the Law applies, so that processing can occur.

The data subject's consent is not the only legal basis for data processing under the LGPD. In fact, in employment relationships consent is unlikely to be the most appropriate basis for processing personal data. Given the imbalance in the parties' positions, it can be argued that any consent by employees was not freely given, which is one of the requirements stipulated by the LGPD for valid consent.

The second point relates to information security, one of the pillars established by the LGPD to ensure that personal data is protected from unauthorized access and improper or illicit processing. Implementing effective information security measures when employees are working on site is challenging enough, but that challenge becomes even tougher in the context of remote work.

In information security, the fundamental step is assessing what administrative and technical measures can be taken to reduce exposure to the information security risks inherent in distance working. Whenever possible, it is preferable for organizations to offer their employees the equipment they need to do their work, and have that equipment configured by the organization's IT specialists, thus providing better protection for the equipment used by employees.

The use of personal equipment increases considerably the risk that unauthorized third parties may access personal data held by the organization, since the organization does not have any way to know if the equipment has been infected by malware, if its antivirus software and other applications are up to date, and if it is used only by the employee.

Another aspect of information security is protecting the confidentiality of personal data that can be accessed by employees. Working from home or in a public place may enable third parties who are not authorized to know certain information (including the employee's family and friends) to obtain access to data simply because they are nearby and can hear a telephone call or see the employee's computer screen.

The duty of confidentiality is implicit in employment relationships, which are based on mutual trust. Violation of that trust constitutes cause for dismissal, according to article 482(g) CLT. Similarly, Law 9279, which governs rights and obligations with respect to intellectual property, makes it a crime to disclose or use, without authorization, confidential information or data obtained by reason of employment, even if the disclosure or use occurred after the termination of employment.

To address these situations, two main recommendations can be made to organizations of all kinds: (i) include confidentiality clauses in employment agreements, or make separate NDAs with employees, highlighting the sensitivity of the information employees will have access to and their obligation not to disclose that information to third parties in any circumstances, on pain of administrative penalties, and (ii) promote awareness of information security through frequent and recurring campaigns so that employees realize how important the matter is for the organization, understand their responsibility for protecting information, and know the best practices for avoiding events that could result in a violation of the LGPD.

This article can be found in the e-book* ***"Current Employment Issues: the end of the pandemic and new ways of working". *Click here to read the whole content.*

› PROFESSIONALS

Professionals who combine legal insight and market perspective

Felipe Palhares