REMOTE WORK AND DATA PROTECTION: HOW DO ORGANISATIONS SECURE PERSONAL DATA PROTECTION COMPLIANCE FROM HOME?

Sofia Ribeiro

University of Porto, Faculty of Engineering, INESC TEC (PORTUGAL)

Abstract

In the Information Society, business processes tend to become increasingly digital and operate in the virtual world. With the recent pandemic, this transformation has become almost mandatory. With their workers performing their duties remotely, organisations feel the need to digitally adapt their processes. Among several aspects of concern in these transmutations, one stands out: data protection. How can data protection be controlled remotely? Workers take to their homes their work equipment, their documents and their information with them - full of personal data. With the entry into force of the GDPR, organisations have a duty to register the treatment of information containing personal data. This requires that information circuits be controlled, i.e., a mapping of business processes and the information contained and transmitted in them. A case study was carried out with focus on the activities of the Data Protection Group of a private Portuguese research and development company in order to discover how an organisation, where the main asset is information, controls and monitors data protection compliance.

Keywords: data protection, GDPR, information security, remote work, digital transformation.

INTRODUCTION

Digital transformation is a phenomenon that has been emerging since the 1990s and since then, namely, with the increase development and use of smart devices and social media platforms, it has only been growing. Vial (2019) defines digital transformation as «*a process that aims to improve an entity by triggering significant changes to its properties through combinations of information, computing, communication, and connectivity technologies"*. In other words, digital transformation describes the digitization and digitalization[16] of work once carried out by individuals in organisations – this digital work includes the use of new technologies and the possibility of working remotely from the place of work and the employer (Nagel, 2020).

Although it has been part of the organisation's lives, with the emergence of the COVID-19 pandemic, digital transformation and its impact on business processes only accelerated. Through voluntary or mandatory (government) restrictions, organisations quickly started to shift their employees to remote work (Nagel, 2020). This led to a massive work transformation with the integration of new technologies, such as virtual desktop infrastructures and Desktop as a Service (DaaS), into the daily lives of many workers (Borkovich & Skovira, 2020; Koehler, Cervini, & Vetter, 2020).

[16] 'Digitization' is here understood as "digitally enabling analog or physical artifacts for the purpose of implementing into said artifacts into business processes with the ultimate aim of acquiring newly formed knowledge (...).", and 'Digitalization' understood as "fundamental changes made to business operations and business models based on newly acquired knowledge gained via value-added digitization initiatives." (Schallmo & Williams, 2018).

The shift to remote work caused by the COVID-19 pandemic required two conditions: a rapid digital transformation of business processes and the transfer of information from the office to the household. Under normal circumstances, these changes are a complex and long process that requires training and awareness programs for workers so that every aspect is covered and secured. However, due to the constraints imposed by the pandemic, this shift was abrupt and, for many organisations too fast; and, as a result of that, relevant aspects were overlooked when informing and raising workers' awareness of this new work environment – one of those is information security, and, with that, data protection (Borkovich & Skovira, 2020; Nagel, 2020).

It becomes important to know how organisations can guarantee the security of their information and the compliance with the General Data Protection Regulation (GPDR) in this new form of decentralised work that goes beyond the office borders. Due to the novelty of this problem, a case study was conducted to answer the following question: "*how do organisations secure personal data protection compliance from home?"*. The object of this case study was a Portuguese R&D *(research and development)* organisation and its Data Protection Group (DPG), specifically how it manages to control and monitor data protection in a remote work environment.

This paper is divided in five sections: an introduction to the overall theme of the paper and the question proposed; a second section detailing the main topic of the paper; a third section describing the methodology used and a brief description of the organisation that was the object of the case study; a forth section with the results, and finally, a fifth section with the conclusions of the case study.

DATA PROTECTION IN THE NEW REMOTE WORK CONTEXT

GDPR and remote work

Thanks to technology and digital transformation, employees can work from the safety of their homes; nonetheless, it needs to be ensured that their new work situation also keeps any accessed and processed data just as protected as if they were in the office.

When the General Data Protection Regulation (GDPR) came into force, in May of 2018, many organisations promptly employed security measures to keep their data secure. Back then, the focus was primarily limited to office boundaries. Now, with the majority of employees working from the comfort of their homes, organisations are forced to reassess their security measures and ensure that compliance with GDPR can still be achieved in this new work environment (Lueck, 2020).

Some organisations already had processes and policies in place that allowed for this remote control and monitoring and now they only have to ensure that those policies are in use by their remote workers. However, many organisations don't have these rules and policies – it becomes necessary to identify if this shift in work environment impacts or changes their risks levels (Lueck, 2020).

To prevent data breaches[17] organisations need to reassess their attitude towards security in order to provide a safe remote work environment. But how do organisations assess the impact of remote working?

[17] Under the GDPR, a personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed" (Škiljić, 2020).

The GDPR institutes a 'Data Protection Impact Assessment' (DPIA)[18] to identify data protection and privacy risks and deal with them accordingly. As Lueck (2020) states, a DPIA can be used to identify and analyse how data privacy may be affected by various activities while working remotely. Organisations are responsible for guaranteeing that the appropriate controls are in place when personal data is accessed or processed from a remote environment, and that the information is not treated differently from that in the office. They must audit the security procedures implemented not only by themselves but also by their service providers and apply adequate measures regarding privacy and data protection, implementing solutions such as privacy from design and standard (Škiljić, 2020).

The integrity and confidentiality of data is a fundamental principle for data processing under the GDPR. To guarantee that personal data is secure and private, appropriate security measures must be put into place. Organisations must consider the increased security risks of operating their workforce remotely – it is vital that all its data is backed up, protected, and easily restored in the event of a breach (Lueck, 2020; Malecki, 2020). Pseudonymisation and encryption are two examples of measures to guarantee confidentiality, integrity, availability and the strength of processing systems and services, as well as measures to restore availability promptly when an incident occurs (Škiljić, 2020). Another one is giving access to information on a "need-to-know" basis (Koehler et al., 2020).

Information security challenges

Even though the focus of this paper is data protection and GDPR compliance, it is indispensable that the topic of information security be addressed. In fact, data protection and information security form a symbiotic relationship – due to the high level of digital transformation of the work environment, one cannot be without the other.

The aim of information security is to protect the resources of an organisation, such as information, computer hardware and software (Peltier, 2014). The increased reliance on technology brought about by the recent pandemic has contributed to greater information security risks. Organisations now more than ever must consider the main threats and risks to information security.

Why is confidential information and personal data so vulnerable when people work from home?

In the current work context, remote access to the organisation's systems and information is essential for remote work to function, applications like file-sharing and collaboration platforms and cloud solutions are heavily used, there are various devices accessing the organisation's network, there's higher email traffic. These might all lead to data breaches if remote access solutions are hastily implemented (Koehler et al., 2020; Škiljić, 2020).

The main threat to an organisation's data and information security is human error. Even if the cause of this human error is of non-malicious intent (Wiley, McCormac, & Calic, 2020), the remote work environment creates quite compelling opportunities for cyber criminals (Škiljić, 2020). And if this issue ordinarily eludes the IT team, it is now worsened by remote work and lack of adequate cyber and information security training for teleworkers (Babbs, 2020; Borkovich & Skovira, 2020; Koehler et al., 2020). Because it is unlikely that all organisations have the means to supply their employees with a work computer, some, if not most, use their personal devices for remote access to the organisation's servers, as well as their private wi-fi networks –

[18] "Where a type of processing in particular using new technologies, (...), is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. (...)" (Article 35, GDPR).

if these are insufficiently secure, they present themselves as potential entry points for cybercriminals (Škiljić, 2020).

Is safe to say that there is a strong need for better cyber and information security policies and planning for teleworkers. As more organisations implement remote working, it is important that security technologies, training, and compliance are in place to ensure the safety of sensitive data. It is required that organisations build awareness to the risks of remote working for information security and implement policies and infrastructures that influence effective privacy practices (Babbs, 2020; Borkovich & Skovira, 2020; Koehler et al., 2020).

But one aspect must not be forgotten: these solutions should not inhibit employees' productivity. Reports have shown that employees will find ways to counter security measures if they get in the way of them doing their jobs (Borkovich & Skovira, 2020). According to the 2020 Tessian Report (Tessian, 2020), 91% of IT leaders trust their workers to follow the best security practices when working remotely, while 52% of employees believe they can get away with riskier behaviour. Within the reasons for not following security practices: 48% goes to not being watched by IT and 47% to being distracted. Also, employees report that security policies are a burden. 84% of IT leaders agree that data loss protection is more difficult when workers are working remotely; 51% say that such policies impair productivity; 58% believe that information is less safe when they work remotely; and 54% of employees find workarounds when security policies stop them from doing their job. As a result, 30% of infringements involve employees exposing business information because of incompetent or malicious actions. Insider threats and loss of data via email are especially tough for IT leaders to monitor due to lack of visibility of the threat. And according to the 2020 Wrike Remote Work Security Survey (Pham, 2020), roughly 41% of workers said they still use personal applications to transmit confidential files on a weekly basis.

METHODOLOGY

To answer the question proposed – *how do organisations secure personal data protection compliance from home?* – it was developed a case study. Case studies investigate a real life phenomenon within its environmental context, which can be an individual, a group, an organisation, an event or a problem (Yin, 2018). Due to its in-dept analysis, a case study is the best tool to gain understanding of the "how" of a situation (Ridder, 2017). This case study has its focus on an R&D organisation and on how its Data Protection Group (DPG) manages to control and monitor data protection in a remote work environment.

The organisation in case is INESC TEC - Institute for Systems and Computer Engineering, Technology and Science, a Portuguese private non-profit research institution, dedicated to scientific research and technological development that counts with over 1200 collaborators spread across research centres and administrative services, and acts as an interface of the academic, business and public sector worlds (INESC TEC, 2020). Looking specifically at the DPG, it is composed of members of the legal team, of the management support team and of the IT services.

To gather information and be aware of the DPG procedures, the following methods were used: observation, documentation analysis, and unstructured interviews.

In this case, the observation was the main source of evidence since the author is part of the DPG of INESC TEC – this is, therefore, characterized as participant observation (Yin, 2018). Regarding the analysis of documentation, it was studied the documentation produced by the DPG in matter of records processing activities and the orientations emitted for *protection personal data and confidential information when working remotely*. It was also analysed the statement about *teleworking remote control* from the Portuguese National Data Protection

Commission (*Comissão Nacional de Proteção de Dados*). The interviews are classified as unstructured since they occurred as informal conversations.

RESULTS

Use of remote work platforms

INESC TEC already had a big degree of digital transformation of its business processes, possessing many applications that allowed remote work such as videoconference platforms (Zoom, Google Hangouts), communications tools (email, VOIP, Mattermost Chat, ticket system), and file-sharing and collaboration tools (Nextcloud Drive, shared folders, Wekan, Office365). It also already had security mechanisms and policies in place to keep its information and data secure, such as regular software updates, installation of antivirus software with frequent scans and updates, systematic backups, information security practices and a culture of consulting the IT services to resolve issues. What mostly changed was the increased degree of use and implementation of these tools, mechanisms, and policies. The symbiosis between information security (especially cybersecurity) and data protection was already great, the shift to remote work only exacerbated this interdependence.

Collaboration tools such as file sharing and videoconferencing platforms have become much more used than before. Although the use of cloud drives or shared folders on INESC TEC's servers is already practically rooted in the everyday work, the use of videoconference platforms was not. The use of these new communication tools was one of the big differences from the pre-pandemic times.

There was also a greater and almost exclusive use of digital documentation. This is due to the need dictated by the work context and facilitated by the tools already in use and the implementation of mechanisms such as digital signatures and certificates. Being intrinsically linked to the public government, the organisation was encouraged to use these mechanisms, since the Portuguese government is well underway to dematerialize the public administration processes, causing public financing entities that work with INESC TEC to implement these dematerialization mechanisms.

It is said "almost exclusive" because, although most national and European project financing initiatives started to employ digital signatures and certificates to carry on their processes, some international initiatives did not, continuing to use the "*in person*" signature of contracts and the communication of these procedures by mail.

The Data Protection Group's work

The main activities of the DPG are record of processing activities, Data Protection Impact Assessments (DPIA), creation and application of data protection policies and measures (the implementation of these policies is still in process), audits and issuing of opinions and recommendations. These activities normally would be carried out by face-to-face meetings and interviews with the services and research centres, but also through "water-cooler" conversations and off the record exchanges. Now they are conducted through videoconference meetings, the INESC TEC chat or through email.

When asked about these meetings and interviews, the group's members remarked the increased effort in their performance since it is more difficult to analyse and study people functions and activities over a videoconference call – the questions have to be more specific and comprehensive to get across what is asked and to understand if anything is being left out. More follow-up meetings are also required. Many times, people's functions and activities are so deeply rooted and performed so naturally that they forget to mention certain details or parts of work processes sometimes important to the DPG job. The DPG also uses these meetings to raise awareness to best practices regarding the handling of sensitive information and personal data.

The DPG's work in relation to adapting the workforce to the teleworking context consisted of assessing the impact of the new tools and platforms and issuing guidelines to reinforce data and information security. These guidelines address the use of *Devices*, *Email*, and *Cloud Network Access* as shownon Table 1. Such orientations are based on already established policies within INESC TEC, guidelines produced by the Portuguese National Data Protection Commission and European statements.

Table 1. Orientations for Protecting Personal Data and Confidential Information when Working Remotely (adaptation from the INESC TEC's guidelines)

Devices	•Take extra care that devices (USBs, phones, laptops, or tablets) are not lost or misplaced. •Ensure that the devices have the necessary updates, (operating system updates and software/antivirus updates) and set up automatic virus scans. •While working remotely keep following the best practices regarding the safety of online navigation, avoiding access to suspicious websites, the download and sharing of possibly infected files or illicit contents. •Ensure the devices are used in a safe location or where they can be in sight, and minimise who else can view the screen, particularly if working with sensitive personal data. •Lock screen of the device if left unattended for any reason. •Make sure the devices are turned off, locked, or stored carefully when not in use. •Use effective access controls (such as passwords or multi-factor authentication) and, where available, encryption to restrict access to the device and to reduce the risk if a device is stolen or misplaced. •When a device is lost or stolen, take steps immediately, informing the organisation services of the occurrence.
Emails	•Use work email accounts rather than personal ones for work-related emails involving personal data. If sharing personal data is necessary, make sure contents and attachments are encrypted, and avoid using personal or confidential data in subject lines. •Before sending an email, ensure it is sent to the correct recipient, particularly for emails involving large amounts of personal data or sensitive personal data.

Cloud and Network Access	•Whenever possible only use the organisation trusted networks and services, such as the organisation Drive, and comply with the organisational rules and procedures about IT resources usage, password management, and data sharing. •Follow the instructions provided by the organisation services concerning the configuration and responsible use of the VPN, and do not forget to turn off the VPN when the remote work is over. •Ensure that any locally stored data is synchronised with the organisation Drive or adequately backed up in a secure manner.

The DPG is also starting to invest more in training and awareness raising for workers, noting that this is the most important component towards ensuring information security and data protection. This is being implemented through online courses made available to the workers through INESC TEC's Moodle (a free, open-source learning management system) and the already mentioned sensibilization during the meeting and interviews regarding the DPG's activities.

DISCUSSION AND CONCLUSIONS

In order to answer the question – *how do organisations secure personal data protection compliance from home?* – a case study was carried out that focused on the Data Protection Group (DPG) of a Portuguese research and development organisation, analysing its documentation and its daily activity in order to better understand how they guarantee control and monitoring of security and data protection. In this paper, a small overview of the topic under discussion was made, where the issues of information security challenges and the role of the GDPR in the new context of work brought about by the pandemic COVID-19 were briefly addressed.

As can be seen, the organisation in study already had, before the pandemic, a high level of digital transformation, having all of its processes in digital mode or, at least, easily adaptable to digital traffic, as well as mechanisms and tools that allow a smoother transition to the remote work, such as several communication and collaboration mechanisms and tools in place that allow working at a distance, while also having security measures and practices such as frequent software updates, use of antivirus software, and a good organisational culture of consulting IT services for problem solving instead of trying to get around them by personal initiative.

The greatest transformation of the DPG's activities was the means by which they take place: from face to-face meetings to video conferencing. This requires greater effort as it becomes more difficult to understand exactly the activities and functions of the workers. This effort is substantiated by more comprehensive questions and follow-up meetings. DPG has also made a greater effort to raise the awareness of workers to keep in mind good information security and data protection practices. This awareness-raising has been carried out alongside meetings within the scope of the group's activities; but also in the development of an online course, through the organisation's Moodle, for the workers.

From this study, one can see that organisations that have a higher level of digital transformation have a greater ease in adapting their data protection processes to the new context of remote work; nonetheless, difficulties are felt with regard to control and monitoring since it requires, on the part of the security and data protection team, a more rigorous and comprehensive inquiry, in addition to the reinforcement of cybersecurity measures. Also, the training and awareness of workers is the most important aspect in guaranteeing information security and data protection since they are in an environment outside the office where the threats and risks are bigger. This allows to answer the question proposed.

So, how do organisations secure personal data protection compliance from home?

Organisations secure data protection compliance through 2 main vectors: an information security and data protection policy, and the training and awareness of the workforce.

The implementation of an information security and data protection policy is the first step in guaranteeing personal data protection compliance and it establishes the organisation's attitude towards information and data, asserting its value as an important asset and propriety of the organisation that needs to be protected from unlawful access, modification, disclosure, and destruction (Peltier, 2014). Additionally, awareness is the key in improving security in the remote workplace and that a strong technical infrastructure is essential (Borkovich & Skovira, 2020).

Several information security measures should be put in place. Organisations must have in mind not only vulnerabilities to their own network and physical storage of data but also those in the transfer of information between the organisation's network to their personal spaces. The GDPR recommends encryption to protect personal data in transit, ensuring privacy, information security and preventing data breaches (Lueck, 2020). According to this risk-based approach by the GDPR, companies must consider security risks in remote work more intensively than under normal circumstances and adapt their security policy (or best practices) to this new environment. Organisations must audit the security measures implemented not only by themselves but also by their service providers and adequate measures must be put in place regarding privacy and data protection, implementing solutions such as privacy from design and standard (Škiljić, 2020). Ensuring the authenticity of digital certificates is also essential for the integrity of the information and data in signed documents and emails.

Workers should be encouraged to automatically save and store their documents and data in a shared area, and not on personal computers. Organisations should have a backup solution and match the frequency of backup with the importance of the data. In addition to protecting the organisation's data, there are a number of additional steps that organisations can take to create and maintain a secure remote work environment, such as (Malecki, 2020):

i. Protecting the infrastructure with strong security protocols: ensuring that all work devices have the appropriate protection measures and a strong VPN connection to the company network is in place;
ii. Protecting the network: through, for example, implementing software that can constantly scan for viruses and suspicious connections;
iii. Encouraging workers to use the IT support team: workers should be encouraged to consult IT support teams about any concerns, rather than trying to resolve technical issues on their own, to ensure that issues are resolved as quickly and safely as possible;
iv. Communicating securely: tools used for company-wide communications must meet recognized security standards;
v. Giving clear guidance to workers on how to protect their devices and networks, as well as training on how to configure security solutions;
vi. Implementing a robust data recovery plan for business continuity.

Additionally, it may be necessary to assess each individual environment. Not all workers in an organisation use personal data in their jobs. The organisation can try to understand the impact of the new remote work environment, gaining insights into which workers access personal data while working at home and subsequently create various risk categories for these workers

(Lueck, 2020). It should be kept in mind, though, since there is no legal provision (in Portugal) that regulates remote control, the general rule of prohibiting the use of means of remote surveillance, in order to control the professional performance of the worker, is fully applicable to the reality of remote work. In fact, the same conclusion would always be reached by applying the principles of proportionality and the minimization of personal data, since the use of such means implies an unnecessary and certainly excessive restriction of the worker's private life (Comissão Nacional de Proteção de Dados, 2020).

ACKNOWLEDGEMENTS

The author would like to thank the INESC TEC Data Protection Group for their contribution and participation in the preparation of this paper.

DECLARATION OF CONFLICT OF INTERESTS

The author reports an investigation grant given by INESC TEC and by the FCT - Fundação para a Ciência e a Tecnologia (Portuguese Science and Technology Foundation) to work with the Data Protection Group and the Management Support Services of INESC TEC.

REFERENCES

Babbs, A. (2020). How to leverage data security in a post-Covid world. *Computer Fraud & Security*, *2020*(10), 8–11. https://doi.org/10.1016/S1361-3723(20)30107-X

Borkovich, D. J., & Skovira, R. J. (2020). Working From Home: Cybersecurity in the Age of Covid-19. *Issues in Information Systems*, *21*(4), 234–246. Retrieved from https://www.iacis.org/iis/2020/4_iis_2020_234-246.pdf

Comissão Nacional de Proteção de Dados. (2020). Orientações sobre o controlo à distância em regime de teletrabalho.

European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and 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), Official Journal of the European Union. Retrieved from: https://eur-lex.europa.eu/eli/reg/2016/679/oj

INESC TEC. (2020). INESC TEC - Institution. Retrieved May 14, 2020, from https://www.inesctec.pt/en/institution

Koehler, T., Cervini, P., & Vetter, J. (2020). The abrupt shift to remote working has amplified cyber security problems. Retrieved from http://eprints.lse.ac.uk/106456/1/usapp_2020_08_22_the_abrupt_shift_to_remote_working_has_amplified.pdf

Lueck, M. (2020). GDPR in the new remote-working normal. *Computer Fraud & Security*, *8*, 14– 16. https://doi.org/10.1016/S1361-3723(20)30086-5

Malecki, F. (2020). Overcoming the security risks of remote working. *Computer Fraud & Security*, *7*, 10–12. https://doi.org/10.1016/S1361-3723(20)30074-9

Nagel, L. (2020). The influence of the COVID-19 pandemic on the digital transformation of work. *International Journal of Sociology and Social Policy*, (ahead-of-print). https://doi.org/10.1108/IJSSP-07-2020-0323

Peltier, T. R. (2014). *Information Security Fundamentals* (Second Edi). CRC Press. Retrieved from https://books.google.pt/books?id=MSPFAAAAQBAJ

Pham, M. (2020). COVID-19 and the Future of Work Security: Is Remote Work Really Secure? Retrieved from https://www.wrike.com/blog/remote-work-security-survey/

Ridder, H. G. (2017). The theory contribution of case study research designs. *Business Research*, *10*(2), 281–305. https://doi.org/10.1007/s40685-017-0045-z

Schallmo, D. R. A., & Williams, C. A. (2018). History of Digital Transformation. In *Digital Transformation Now! Guiding the Successful Digitalization of Your Business Model* (pp. 3–8). Cham, Switzerland: Springer Nature. https://doi.org/10.1007/978-3-319-72844-5_2

Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats. *International Cybersecurity Law Review*, *1*(1–2), 51–61. https://doi.org/10.1365/s43439- 020-00014-3

Tessian. (2020). The State of Data Loss Prevention: Why DLP Has Failed and What the Future Looks Like. Retrieved from https://www.tessian.com/research/the-state-of-data- loss-prevention-2020/

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Los Angeles: SAGE. https://doi.org/10.1177/109634809702100108