Ogletree Deakins

Employers & Lawyers. Working Together

Protection of physical and logical personal data in a remote work context

Virtual Vigitrust Global Advisory Board

Thursday September 24th , 2020

Speakers

Cécile Martin
Managing Partner

Direct: +33 1 70 61 24 06
Mobile: +33 7 89 48 39 64
cecile.martin@ogletree.com

Thibaud Lauxerois
Associate

Direct: +33 11 82 88 39 80
Mobile: +33 7 64 42 25 88
thibaud.lauxerois@ogletree.com

Ogletree Deakins

Introduction

- Hacking risks cause 50% of the data breaches.
- Accidental breaches constitute 23% of data breaches.
- Both these risks are increased by remote work.

- In France remote working can only be arranged:
  - on a consensual basis with the employee according to either a collective bargaining agreement or a charter.
  - by exception, without the employee's consent, when exceptional circumstances occur.
    - These exceptional circumstances may include an epidemic or other force majeur events.
    - Even though a charter is not mandatory, it is strongly advisable to draft one in order to exactly determine the employee's rights and obligation in this new context.

Applicable principles

- Article 25 of the GDPR : data protection by design and default
  - All aspects of data protection need to be set up prior to implementing remote work.

  ➢ It is necessary to the implementation of remote work in advance, and companies cannot wait for a second lockdown to implement security measures.

- Article 32 of the GDPR : security of processing
  - "*Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*"

  ➢ A specific context such as unprepared remote working may justify applying lower security standards, but only to a small extent and for a short duration.

Securing the software

- Equip all employees' workstations with a firewall, anti-virus software and a tool blocking access to malicious sites.

- Set up a Virtual private network to which employees must connect prior to accessing professional data.

- Provide employees with appropriate working and communication tools guaranteeing the confidentiality of exchanges and shared data.

  - ➢ Analyse the Terms of Use of each app before implementing it.

  - ➢ Check the data is not going to be re-used and is erased after it is no longer useful to running the app.

  - ➢ Keep the software up to date.

Setting up a charter

- A charter must be drafted and circulated in such a way that it becomes enforceable against employees in case of a violation.

  - The charter must remind customary safety reflexes (password, caution against phishing, other scam emails…)

  - The charter must include specific instructions on remote working (router's internal software, Wi-Fi encryption…)

  - Give access to IT support and an emergency contact in case of a serious situation occurring (loss, theft…)

Training employees

- Organize employees training sessions featuring:
  - ➢ Explanations on the reasons why they are expected to ensure the security of the data.
  - ➢ Details on the security measures expected from them.
  - ➢ Examples of behaviors to adopt based on actual situations.
  - ➢ Tests to verify each employee's proper understanding with a minimum result requirement.

Managing employees' personal devices

- Some companies were unable to acquire enough laptops for all their employees before the lockdown.
- In this context, the employer must resort to letting the employee use their own device.
- However, the employer is limited in its capacity to set up security software on an employee's device.
  - ➢ It is advisable to limit BYOD to employees with recent, up-to-date software and the necessary protection software.
  - ➢ The employer may consider making employees with inadequate devices prioritary to benefit from newly-bought devices.
  - ➢ If necessary, exempting employees from work may be the only solution to remain compliant.

Preserving employees' rights

- The employer cannot monitor a remote worker's computer activity further than necessary.
  - For instance, the employer cannot set up monitoring tools to ensure that employees are actually working (keyloggers, webcams etc.)
- When an employee uses their personal device for professional purposes, they are also expected to use it for purely personal purposes, with which the employer cannot interfere.
  - The safety measures cannot be such that they prevent the employee from freely browsing the web or downloading new apps.
  - The employer cannot try and have access to the employee's personal files and correspondance.

Acting upon a breach

- In case of a data breach :
  - Notify the data protection authority within 72 hours of becoming aware of it.
  - If required, notify data subjects.

- Consequences of a data breach:
  - Reputational damage,
  - Fine up to 10,000,000 EUR, or 2 % of the total worldwide annual turnover of the preceding financial year,
  - Enforcement of additional security measures under the supervision of the enforcers.

➢ In order to make employees accountable for their negligence or misconduct, disciplinary sanctions against faulty employees must be considered.

Thank you

Paris / Berlin / London / Chicago / Los Angeles / New York
and 48 offices in the United States, in Canada and in Mexico

+33 1 86 26 27 42

www.ogletree.fr

Ogletree Deakins