

## Fact sheet

# Protecting employee's private life

**“Working from home or shared spaces presents unique challenges for employee privacy. Unlike controlled office environments, home offices vary dramatically in terms of infrastructure, physical security, and network reliability.**



Employees' private life encompasses their personal activities, relationships, and communications conducted outside the workplace (Ranc, 2020). This concept is protected under various legal frameworks, notably Article 8 of the European Convention on Human Rights, which guarantees the right to respect for private and family life. In the workplace, this right extends to personal communications and activities, even during working hours, provided they do not interfere with professional duties (Markham, 2024). The French legal system, for instance, recognises this distinction, allowing employers to access professional files but not personal ones without consent or specific legal grounds.

It seems very important to safeguard employees' personal data and privacy, whether they are working on-site or remotely. However, it appears that data protection becomes more complex in remote working environments, as organisations may lack comprehensive information or access regarding the methods employees use to connect remotely.

In that context, a study by IBM Security (2022) highlighted that 83% of organisations experienced more than one data breach, with remote work contributing to higher breach costs. These risks stem from vulnerabilities in home networks, unencrypted communications, and the growing use of personal devices (BYOD – Bring Your Own Device), often outside the control of IT departments. In such decentralised environments, protecting employee privacy becomes both a technical and ethical imperative.

## Challenges of protecting employees **private life in HRW**

Working from home or shared spaces presents unique challenges for employee privacy. Unlike controlled office environments, home offices vary dramatically in terms of infrastructure, physical security, and network reliability. Employees may use insecure Wi-Fi connections, fail to install regular software updates, or even share their workspace with others, increasing the risk of accidental data leaks.

The increasing use of monitoring and productivity tracking tools, such as keystroke loggers, webcam surveillance, or application usage trackers, has sparked significant debates. While such tools may serve managerial purposes, they often infringe on personal privacy boundaries, especially when employees work from spaces where personal and professional lives overlap.

As illustrated in the figure below, remote work environments often include multiple devices, cloud-based applications, and connections to unsecured networks, each presenting potential vectors for privacy violations.



Academic literature has thoroughly examined the implications of remote work on employee privacy.

A significant concern is the blurring of personal and professional spheres, which undermines the right to a private life as protected by Article 8 of the European Convention on Human Rights.

According to Ajunwa et al. (2017), employee monitoring in the digital

age raises critical concerns about autonomy and dignity, particularly when surveillance continues outside of regular office hours. Similarly, Nissenbaum's (2004) theory of contextual integrity posits that privacy violations occur when data flows deviate from their expected context, which is a frequent occurrence in remote work scenarios.

## Solutions and recommendations for HR and managers

Addressing employee privacy in remote and hybrid contexts requires a strategic approach that balances operational control with respect for individual rights. Below are some key recommendations for HR professionals and managers:

1

### **Develop clear and transparent policies**

Ensure that any data collection or monitoring is explicitly documented, justified, and communicated. Employees should be informed of what data is collected, how it is stored, who accesses it, and for what purpose.

2

### **Apply the principle of data minimisation**

Collect only the data necessary to achieve clearly defined objectives. Avoid intrusive practices such as webcam activation or GPS tracking unless absolutely required and consented to.

3

### **Strengthen IT and security infrastructure**

Invest in secure VPNs, endpoint security, multi-factor authentication, and encrypted communications. Encourage regular updates and offer support for home office configurations.

4

### **Respect boundaries and work-life balance**

Avoid surveillance outside of agreed working hours. Allow flexibility and focus on outcomes rather than constant visibility. Implement a "right to disconnect" policy to preserve employee wellbeing.

5

### **Train managers in privacy-aware leadership**

Equip team leaders with the knowledge and tools to foster trust-based cultures rather than control-based approaches. According to CIPD (2022), leadership style greatly influences how privacy measures are perceived and respected.

6

### **Conduct regular privacy impact assessments (PIA)**

Evaluate the impact of new technologies or processes on employee privacy before deployment. Include employees in the consultation process to ensure transparency and co-ownership.



## Recommended Resources

---

### Video

- "The Right to Disconnect from work" – A comprehensive overview of the legal and ethical considerations surrounding employees' right to disconnect and protect their private lives. [https://multimedia.europarl.europa.eu/en/video/the-right-to-disconnect-from-work\\_N01-AFPS-210119-RTDI](https://multimedia.europarl.europa.eu/en/video/the-right-to-disconnect-from-work_N01-AFPS-210119-RTDI)

### Further reading

- Bai, A., & Vahedian, M. (2023). Beyond the Screen: Safeguarding Mental Health in the Digital Workplace Through Organizational Commitment and Ethical Environment. arXiv. [arxiv.org](https://arxiv.org)
- Choudhury, P., Larson, B. Z., and Foroughi, C., 2021. Is it time to let employees work from anywhere? Harvard Business Review. [online] Available at: <https://hbr.org/2021/08/is-it-time-to-let-employees-work-from-anywhere>

### Bibliography

- Ajunwa, I., Crawford, K. and Schultz, J., 2017. Limitless worker surveillance. California Law Review, 105(3), pp.735–776. <https://doi.org/10.2139/ssrn.2746211>
- Ranc, S. (2020). Respect for personal life in the workplace during working hours: the inspection of employee computer files. Revue de droit comparé du travail et de la sécurité sociale.
- Markham, I. (2024). Employee Data: 5 Ways to Tighten Security to Shore Up Trust. The Wall Street Journal.
- Nissenbaum, H., 2004. *Privacy as contextual integrity*. Washington Law Review, 79(1), pp.119–157. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>