

Das Privatlebens der Mitarbeitenden schützen

„Die Arbeit von zu Hause oder aus gemeinsam genutzten Räumen stellt besondere Herausforderungen für die Privatsphäre der Mitarbeiter dar. Im Gegensatz zu kontrollierten Büroumgebungen unterscheiden sich Heimbüros erheblich in Bezug auf Infrastruktur, physische Sicherheit und Netzwerkzuverlässigkeit.“



Einleitung

Das Privatleben der Mitarbeitenden umfasst ihre persönlichen Aktivitäten, Beziehungen und Kommunikationen, die außerhalb des Arbeitsplatzes stattfinden (Ranc, 2020). Es ist durch verschiedene Rechtsrahmen geschützt, insbesondere durch Artikel 8 der Europäischen Menschenrechtskonvention, der das Recht auf Achtung des Privat- und Familienlebens garantiert. Am Arbeitsplatz erstreckt sich dieses Recht auf persönliche Mitteilungen und Aktivitäten, auch während der Arbeitszeit, sofern sie nicht mit beruflichen Pflichten kollidieren (Markham, 2024). Das französische Rechtssystem, zum Beispiel, erkennt diese Unterscheidung so an, dass es Arbeitgebern den Zugang zu beruflichen Dateien gestattet, nicht aber zu personenbezogenen Dateien ohne Zustimmung oder bestimmte Rechtsgrundlagen.

Es ist sehr wichtig, die persönlichen Daten und die Privatsphäre der Mitarbeitenden zu schützen - unabhängig davon, ob sie vor Ort oder aus der Ferne arbeiten. Der Datenschutz in Remote-Arbeitsumgebungen wird aber immer komplexer, da Unternehmen möglicherweise keine umfassenden Informationen oder keinen Zugang zu den Methoden haben, mit denen sich Mitarbeitende aus der Ferne verbinden.

In diesem Zusammenhang ergab eine Studie von IBM Security (2022), dass 83 % der Unternehmen mehr als eine Datenschutzverletzung erlebten, wozu besonders Remote-Arbeit beitrug. Diese Risiken ergeben sich aus Schwachstellen in Heimnetzwerken, unverschlüsselter Kommunikation und der zunehmenden Nutzung persönlicher Geräte (BYOD – Bring Your Own Device), die oft außerhalb der Kontrolle der IT-Abteilungen liegen. In dezentralen Umgebungen wird der Schutz der Privatsphäre der Mitarbeitenden sowohl zu einer technischen als auch zu einer ethischen Herausforderung.

Herausforderungen beim Schutz des Privatlebens von Beschäftigten in HRW

Die Arbeit von zu Hause aus oder in gemeinsam genutzten Räumen stellt einzigartige Herausforderungen für die Privatsphäre der Mitarbeitenden dar. Im Gegensatz zu kontrollierten Büroumgebungen unterscheiden sich Home-Offices stark in Bezug auf Infrastruktur, physische Sicherheit und Netzwerkzuverlässigkeit. Mitarbeitende könnten unsichere WLAN-Verbindungen verwenden, regelmäßige Software-Updates nicht installieren oder sogar ihren Arbeitsbereich mit anderen teilen, was das Risiko versehentlicher Datenlecks erhöht.

Der zunehmende Einsatz von Überwachungs- und Produktivitätsverfolgungstools wie Keyloggern, Webcam-Überwachung oder Trackern für die Anwendungsnutzung hat erhebliche Debatten ausgelöst. Während solche Tools Managementzwecken dienen, verletzen sie oft die Grenzen der Privatsphäre, insbesondere wenn Mitarbeitende in Räumen arbeiten, in denen sich Privat- und Berufsleben überschneiden.



Wie in der folgenden Abbildung dargestellt, umfassen Remote-Arbeitsumgebungen häufig mehrere Geräte, Cloud-basierte Anwendungen und Verbindungen zu ungesicherten Netzwerken, die jeweils potenzielle Vektoren für Datenschutzverletzungen darstellen. In der wissenschaftlichen Literatur wurden die Auswirkungen von Remote-Arbeit auf die Privatsphäre der Mitarbeiter gründlich untersucht. Ein großes Problem ist die Verwischung von persönlicher und beruflicher Sphäre, die das Recht auf Privatleben, wie es durch Artikel 8 der Europäischen Menschenrechtskonvention geschützt ist, untergräbt.

Laut Ajunwa et al. (2017) wirft die Überwachung von Mitarbeitenden im digitalen Zeitalter kritische Bedenken hinsichtlich Autonomie und Würde auf, insbesondere wenn die Überwachung außerhalb der regulären Bürozeiten fortgesetzt wird. In ähnlicher Weise postuliert Nissenbaums Theorie der kontextuellen Integrität (2004), dass Datenschutzverletzungen auftreten, wenn Datenflüsse von ihrem erwarteten Kontext abweichen, was in Remote-Arbeitsszenarien häufig vorkommt.

Lösungen und Empfehlungen für HR und Führungskräfte

Der Schutz der Privatsphäre der Mitarbeitenden in Remote- und Hybridkontexten erfordert einen strategischen Ansatz, der die betriebliche Kontrolle mit der Achtung der individuellen Rechte in Einklang bringt. Im Folgenden finden Sie einige wichtige Empfehlungen für HR-Fachleute und -Manager*innen:

1

Klare und transparente Richtlinien entwickeln

Stellen Sie sicher, dass jede Datenerfassung oder -überwachung explizit dokumentiert, begründet und kommuniziert wird. Die Mitarbeitenden sollten darüber informiert werden, welche Daten erhoben werden, wie sie gespeichert werden, wer zu welchem Zweck darauf zugreift.

2

Grundsatz der Datenminimierung

Sammeln Sie nur die Daten, die zur Erreichung klar definierter Ziele erforderlich sind. Vermeiden Sie aufdringliche Praktiken wie die Aktivierung von Webcams oder GPS-Tracking, es sei denn, dies ist absolut erforderlich und erfolgt unter Zustimmung.

3

Stärkung der IT- und Sicherheitsinfrastruktur

Investieren Sie in sichere VPNs, Endpunktsicherheit, Multi-Faktor-Authentifizierung und verschlüsselte Kommunikation. Fördern Sie regelmäßige Updates und bieten Sie Unterstützung für Home-Office-Konfigurationen.

4

Respekt für Grenzen und Work-Life-Balance

Vermeiden Sie Überwachung außerhalb der vereinbarten Arbeitszeiten. Ermöglichen Sie Flexibilität und konzentrieren Sie sich auf Ergebnisse statt auf ständige Transparenz. Beachten Sie das "Recht auf Nichterreichbarkeit", um das Wohlbefinden der Mitarbeitenden zu erhalten.

5

Schulung von Führungskräften in datenschutzbewusster Führung

Statten Sie Teamleiter*innen mit dem Wissen und den Werkzeugen aus, um vertrauensbasierte Kulturen anstelle von kontrollbasierten Ansätzen zu fördern. Laut CIPD (2022) hat der Führungsstil einen großen Einfluss darauf, wie Datenschutzmaßnahmen wahrgenommen und respektiert werden.

6

Durchführung regelmäßiger Datenschutz-Folgenabschätzungen (PIA)

Bewerten Sie die Auswirkungen neuer Technologien oder Prozesse auf die Privatsphäre der Mitarbeitenden vor der Verwendung. Beziehen Sie die Mitarbeitenden in den Konsultationsprozess ein, um Transparenz und Mitverantwortung zu gewährleisten.



Empfohlene Ressourcen

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

Weiterführende Literatur

- Bai, A., & Vahedian, M. (2023). Beyond the Screen: Safeguarding Mental Health in the Digital Workplace Through Organizational Commitment and Ethical Environment. arXiv. 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>

Quellen

- 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/>