**Datenschutz im Arbeitsverhältnis: wie vermeidet man Sanktionen?**

*von Raluca Bădilă, Avocat (Rechtsanwältin RO)*

2026 verhängte die rumänische Datenschutzaufsichtsbehörde (ANSPDCP) konsequent Sanktionen gegen Arbeitgeber, die gegen Vorschriften zur Verarbeitung personenbezogener Daten verstießen.

Die Behörde kann den Verantwortlichen zusätzlich Abhilfemaßnahmen anordnen, u.a. dazu, Betroffene zu benachrichtigen, die Verarbeitung rechtskonform zu gestalten, einzuschränken oder zu unterlassen, die Daten zu löschen, den Datenfluss in Drittländer auszusetzen, etc.

Wir empfehlen, bei der Umsetzung der Maßnahmen, deren Verstöße in der Vergangenheit zu den meisten Sanktionen geführt haben, insbesondere die folgenden Bedingungen zu sichern:

- **Arbeitnehmerüberwachung (Video, Audio, E-Mail, GPS)**
  - Jede Form der Überwachung erfordert ein dokumentiertes berechtigtes Interesse (Risikobewertung – LIA/DPIA);
  - Umfassende und ausdrückliche Vorab- Information der Arbeitnehmer;
  - Der in der Informationserklärung genannte Zweck umfasst ggf. auch die Verwendung im Rahmen von Disziplinarverfahren.
  - Dokumentierte Anhörung der Gewerkschaft oder der Arbeitnehmervertreter;
  - Sammlung von Argumenten, wonach weniger einschneidende Maßnahmen den angestrebten Zweck nicht erreicht haben;
  - Ausschluss von Umkleiden, Toiletten, Essbereichen oder anderen privaten Bereichen bei der Videoüberwachung;
  - Aufbewahrung von Aufzeichnungen für maximal 30 Tage vorbehaltlich begründeter Ausnahmefälle;

*Praxis:* Geldbuße von mehr als 15.000 RON wegen des Einsatzes von Bodycams zur Überprüfung der Einhaltung von Arbeitsschutzvorschriften im März 2026. Dies wurde als zu starker Eingriff in die Privatsphäre angesehen. Sanktion auch wegen der Verwendung von Videoaufnahmen in einer Disziplinaruntersuchung.

- **Biometrische Daten (Fingerabdrücke, Gesichtserkennung)**
  - Zeiterfassung und der Zugang zu den Räumlichkeiten lassen sich nicht durch weniger eingreifende Mittel wie Zugangskarten, PINs oder eine Zeiterfassungs-App gewährleisten;
  - Es liegt eine Rechtsgrundlage gemäß Art. 9 DSGVO vor, und es wurde eine Datenschutz-Folgenabschätzung durchgeführt.

*Praxis:* Geldbuße von 5.000 EUR wegen Verwendung einer fingerabdruckbasierten Zeiterfassung im September 2026. Verpflichtung zu einer Ersatzlösung ohne biometrische Daten.

- **Anträge von Arbeitnehmern (Auskunft, Löschung, Widerspruch)**
  - Es gibt ein schriftliches Antwortverfahren und einen Zuständigen hierfür;
  - Anfragen werden nachweislich innerhalb von 30 Tagen beantwortet;
  - HR- Mitarbeiter sind geschult, Anträge gemäß DSGVO auch dann zu erkennen, wenn diese nicht ausdrücklich als solche formuliert sind.

*Praxis:* Im Oktober 2026 wies die ANSPDCP einen Verantwortlichen an, angeforderte Telefonaufzeichnungen und Videoaufnahmen herauszugeben und seine Verfahren zu überprüfen.

- **Sicherheit und Zugriff auf HR- Daten**
  - Der Zugriff auf Personalakten und Gehaltsabrechnungen erfolgt nach dem „Need-to-know"-Prinzip, d. h. ausschließlich an Personen, deren Aufgaben dies erfordern;
  - Administratorkonten nutzen Multi-Faktor-Authentifizierung (MFA), der Fernzugriff erfolgt per VPN;
  - Testumgebungen (z.B. neue Lohnabrechnungssoftware) verwendet ausschließlich Dummy-Daten;
  - Der Zugriff wird protokolliert;
  - Regelmäßige und dokumentierte Arbeitnehmerschulungen.

*Praxis:* Geldbuße von 8.000 EUR, nachdem ein Administratorkonto gehackt worden war, und Verpflichtung, VPN und MFA einzuführen, Oktober 2026. Auch die Verwendung von Echtdaten bei Tests wurde sanktioniert.

- **Lieferanten und Auftragnehmer**
  - Mit den Dienstleistern für Sicherheit, Lohnbuchhaltung, Arbeitsmedizin, HR-Plattformen etc. bestehen Auftragsverarbeitungsverträge (DPA) nach Art. 28 DSGVO;
  - Die Verträge sehen Schulungen und Zugangskontrollen für das Personal des Lieferanten vor.

*Praxis:* Geldbuße von 2.000 EUR gegen das Sicherheitsunternehmen eines Einzelhändlers, nachdem ein Mitarbeiter einem Dritten Zugang zum Überwachungsraum gewährt hatte.

- **Datenschutzverletzungen**
  - Es gibt ein internes Verfahren, wonach die ANSPDCP innerhalb von 72 Stunden benachrichtigt wird;
  - Es gibt ein Verzeichnis von Vorfällen, auch der nicht gemeldeten;
  - Die Arbeitnehmer sind über relevante Vorfälle und die Meldepflicht geschult.

- **Tarifvertrag und Betriebsordnung**
  - Betriebsordnung und Tarifvertrag regeln keine Datenverarbeitung, die mit der DSGVO unvereinbar ist. Laut EuGH darf eine Vereinbarung mit Arbeitnehmervertretern den Standard der DSGVO nicht herabsetzen.

➢ **Beweismittel, interne Ermittlungen**

- Der Zugriff auf E- Mails oder Konten von Arbeitnehmern bei internen Untersuchungen erfolgt aufgrund eines diesen schriftlich bekanntgegebenen Verfahrens;
- Auf private Konten der Arbeitnehmer erfolgt kein Zugriff.

Im Juni 2026 entschied der EuGH zwar, dass entgegen der DSGVO erhobene Beweismittel nicht automatisch vom Verfahren ausgeschlossen sind. Der Arbeitgeber muss jedoch mit Geldbußen und Schadenersatzansprüchen deswegen rechnen.

**Kontakt und weitere Informationen:**

**STALFORT Legal. Tax. Audit.**
Bukarest – Bistrița – Sibiu

**Büro Bukarest:**
T.: +40 – 21 – 301 03 53
F: +40 – 21 – 315 78 36
M: bukarest@stalfort.ro
**www.stalfort.ro**