Workplace Investigations

Contributing Editors

Phil Linnard at Slaughter and May
Clare Fletcher at Slaughter and May

07. What data protection or other regulations apply when gathering physical evidence?

Switzerland

Author: *Laura Widmer, Sandra Schaffner*
at Bär & Karrer

The Swiss Federal Act on Data Protection applies to the gathering of evidence, in particular such collection must be lawful, transparent, reasonable and in good faith, and data security must be preserved.[1]

It can be derived from the duty to disclose and hand over benefits received and work produced (article 321b, Swiss Code of Obligations) as they belong to the employer.[2] The employer is, therefore, generally entitled to collect and process data connected with the end product of any work completely by an employee and associated with their business. However, it is prohibited by the Swiss Criminal Code to open a sealed document or consignment to gain knowledge of its contents without being authorised to do so (article 179 et seq, Swiss Criminal Code). Anyone who disseminates or makes use of information of which he or she has obtained knowledge by opening a sealed document or mailing not intended for him or her may become criminally liable (article 179 paragraph 1, Swiss Criminal Code).

It is advisable to state in internal regulations that the workplace might be searched as part of an internal investigation and in compliance with all applicable data protection rules if this is necessary as part of the investigation.

---

[1] Simona Wantz/Sara Licci, Arbeitsvertragliche Rechte und Pflichten bei internen Untersuchungen, in: Jusletter 18 February 2019, N 52.

[2] Claudia Fritsche, Interne Untersuchungen in der Schweiz, Ein Handbuch für Unternehmen mit besonderem Fokus auf Finanzinstitute, p. 148.

Last updated on 15/09/2022

Thailand

Author: *Ratthai Kamolwarin, Norrapat Werajong*

at Chandler MHM

The basic premise is that all evidence is admissible unless it violates the law of admissibility and production of evidence, which may vary depending on the jurisdiction. In a criminal court, for example, evidence gathered in violation of the fruit of the poisonous tree doctrine would be typically inadmissible, yet in a civil court, this doctrine would not be an exclusionary rule.

The Personal Data Protection Act, BE 2562 (2019) (PDPA), which is the main data protection law in Thailand, applies when collecting, using, and disclosing pieces of evidence containing the personal data of employees. If the investigation requires sensitive information of the employee under investigation, for example, race, ethnic origin, political opinion, religious or philosophical beliefs, sexual behavior, criminal records, health data, disability, genetic data and biometric data, consent from the employee should be obtained.

Last updated on 15/09/2022

United Kingdom

Author: *Phil Linnard, Clare Fletcher*
at Slaughter and May

Most forms of workplace surveillance involve the processing of personal data that is regulated by the UK GDPR and DPA 2018. The UK GDPR requires that personal data must be processed lawfully, fairly and in a transparent manner; it also must be adequate, relevant and limited to what is necessary concerning the purposes for which it is processed.

Employers should ensure that they have undertaken a data protection impact assessment (DPIA) to document the lawful basis for processing data, and informed employees that their files may be searched before proceeding. They should also ideally have a clear policy on the use of electronic communications systems, detailing when, how and for what purpose they may be monitored by the employer. In Q3 2023 the ICO produced new guidance on monitoring workers (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/employment/monitoring-workers/) and on email and security (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/email-and-security/) which employers should bear in mind during investigations. Employers should also be prepared to make the data collected through employee monitoring available to employees, should the employee submit a data subject access request under the DPA 2018.

The IPA 2016 makes it unlawful in certain circumstances to intercept a communication (such as one on an employer’s telephone or computer network) in the course of its transmission in the UK. The IPA Regs 2018 set out the circumstances where, in a business context, such interception will be lawful. These include monitoring or recording communications without consent to: establish the existence of facts; ascertain compliance with the regulatory or self-regulatory practices or procedures relevant to the business; ascertain or demonstrate standards which are or ought to be achieved by persons using the system; and prevent or detect crime.

Covert surveillance can lead to a breach of an employee's right to privacy under the HRA 1998. The employer will need to consider if covert surveillance is proportionate, which will depend on the facts of each case. Employers should be careful not to use the investigation as an excuse to undertake a "fishing expedition", and should avoid gathering material that is obviously personal, such as private messages and diary entries (see question 8).

Last updated on 27/11/2023

Contributors

Switzerland

Laura Widmer
Sandra Schaffner
Bär & Karrer

Thailand

Ratthai Kamolwarin
Norrapat Werajong
Chandler MHM

United Kingdom

Phil Linnard
Clare Fletcher
Slaughter and May