

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?



South Korea

Author: *Hyunjae Park, Paul Cho, Jihay Ellie Kwack, Kyson Keebong Paek*
at Kim & Chang

It may be difficult for a company to search and collect physical items that personally belong to the employee.

While the company may search and gather electronic data, such as emails or files stored in work laptops or company servers, there are requirements and restrictions under the Criminal Code, the Personal Information Protection Act (PIPA), and the Act on Promotion of Information and Communications Network Utilisation and Information Protection, etc (Network Act), among other laws.

Article 316(2) of the Criminal Code states that accessing the contents of another person's documents, pictures, special media records, etc, that are sealed or designated as secret using technical means may constitute the crime of accessing electronic records.

Under the PIPA, consent must be obtained from the information owner to collect or use personal information, or to provide such information to a third party. Consent must be separately obtained for sensitive information or unique identification information. There are strict requirements as to the format and contents of the consent forms under the PIPA.

The Network Act prohibits accessing an information and communications network without rightful authority or any intrusion that goes beyond the permitted authority for access. Although this may not be an issue if a company directly manages the email accounts at issue, if an employee's email account is protected by a password or through other means, accessing emails from that account without obtaining the employee's consent could constitute unlawful intrusion under the Network Act as well as under the Criminal Code as discussed above.

Last updated on 15/09/2022



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

Contributors



South Korea

Hyunjae Park
Paul Cho
Jihay Ellie Kwack
Kyson Keebong Paek
Kim & Chang



Switzerland

Laura Widmer
Sandra Schaffner
Bär & Karrer