Workplace Investigations

Contributing Editors

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

08. Can the employer search employees' possessions or files as part of an investigation?

Australia

Author: *Joydeep Hor, Kirryn West James, Chris Oliver*
at People + Culture Strategies

The starting position is that there is no general right for an employer to search an employee's possessions. However, an employer may be able to undertake a search in circumstances where:

- the employee consents to the search;
- there is a "right to search" contained in a contract, policy, procedure or industrial instrument; or
- the request to search constitutes a lawful and reasonable direction.

If an employee agrees to a search of their possessions, this consent should be confirmed in writing. If the employee does not consent then the employer can issue a direction to the employee. If the direction is lawful and reasonable, and the employee does not comply, then disciplinary action may be considered.

Last updated on 15/09/2022

Austria

Author: *Michaela Gerlach, Sonia Ben Brahim*
at GERLACH

In general, it is advisable to back up data, documents, emails and other records promptly to prevent their deletion. Admissibility depends on whether the data originates from personal or professional records and whether they are legally relevant. If internal investigations are carried out based on a specific suspicion of a criminal offence, it is the processing of legally relevant data. In general, the processing of professional emails or documents is permissible. If there is no professional connection, access to private files and documents is only permitted in exceptional cases.

If, for example, using a business email account for private purposes is not allowed, the employer can usually assume that the data processed is only "general" data within the meaning of article 6 GDPR and that such data processing is justified by a balancing of interests. However, if private use is allowed, the data may still be part of a special category within the meaning of article 9 GDPR. In such cases, the justification for its use must be based on one of the grounds explicitly mentioned in article 9(2) GDPR.

The employer must protect the employee's rights under section 16 of the ABGB and must consider the proportionality of the interference. Only the least restrictive means – the method that least interferes with the employee's rights – may be used to obtain the necessary information. The employer's interest in obtaining the information must outweigh the employee's interest in protecting his or her rights. The implementation or initiation of controls by the employer does not automatically constitute an interference with personal rights, as being subject to the employer's rights of control is part of the position as an employee.

Last updated on 29/09/2023

Belgium

Author: *Nicolas Simon*
at Van Olmen & Wynant

The employer is, in principle, not entitled to search the employee’s private possessions, except with the explicit consent of the employee. Digital files on the computer or laptop of an employee can be searched under the rules of CBA No. 81 (see question 7) and other privacy rules.

Last updated on 15/09/2022

Brazil

Author: *Patricia Barboza, Maury Lobo*
at CGM

No; employers are only generally allowed to search the work tools they provide to employees, such as company mobile phones, electronic files, and company email and other electronic communications. However, they may also request that employees turn over any company documents in their possession.

Searches of employees’ private possessions or files during an investigation can only occur with the verifiable consent of the employee.

Last updated on 14/09/2023

China

Author: *Leo Yu, Yvonne Gao, Tracy Liu, Larry Lian*
at Jingtian & Gongcheng

Article 13 of the Constitution of the PRC provides that the lawful private property of the citizens shall not be violated. Therefore, during the process of investigation, without the employees' consent, the employer has no right to search the employees' personal possessions or files. If it is necessary to search the employees' personal possessions or files, the employer may require the employees to sign a Letter of Informed Consent before searching; or the employer may call the police and the search will be conducted under the escort of the public security authorities or directly by the public security authorities.

Last updated on 29/11/2023

Finland

Author: *Anu Waaralinna, Mari Mohsen*

at Roschier

Only the police can search employees' possessions (assuming that the prerequisites outlined in the legislation are met).

Last updated on 15/09/2022

France

Author: *Pascale Lagesse, Valentino Armillei*
at Bredin Prat

In internal investigations, the fundamental rights and freedoms of employees are at stake, including the right to privacy, respect for the privacy of home life and correspondence, freedom of expression, and the obligation of loyalty in searching for evidence.

In principle, work emails and files can be reviewed, even without the employee's consent, prior knowledge or warning. This includes: work email accounts; files stored on a work computer or a USB key connected to a work computer; and SMS messages and files stored on a work mobile phone and documents stored in the workplace unless they are labelled as “personal”. On the other hand, it is not permissible for an employer (or an investigator) to review “personal” emails and files, such as documents or emails identified as “personal” by the employee, or personal email accounts (Gmail, Yahoo, etc), even if accessed from a work computer.

There are certain exceptions to the above principle. An employer is allowed to check “personal” emails or data in any of the following cases:

- if the employee is present during the review;
- if the employee is absent, but was duly notified and invited to be present;
- if there is a particularly serious “specific risk or event”;
- if the review is authorised by a judge (this means having to prove a legitimate reason justifying not informing the employee).

When documents or emails are not marked as “personal” but contain information of a personal nature, the employer may open and review the data but may not use such documents or emails to justify applying disciplinary measures to the employee or use such documents or emails as evidence in court if they indeed relate to the employee’s private life.

Special attention must be given to employee representatives who must be entirely free to carry out their duties.

Last updated on 15/09/2022

Germany

Author: *Hendrik Bockenheimer, Susanne Walzer, Musa Müjdeci*
at Hengeler Mueller

Files and documents that are purely business-related – whether in physical or digital form – may, in principle, be inspected by the employer without restriction. The employee has no right to refuse inspection.

When searching business laptops, computers, phones and e-mail accounts, a distinction must be made as to whether private use is permitted (or at least tolerated) or not: if the employee is allowed to use the items exclusively for business purposes, the employer may monitor and control them. If private use is permitted, the employee's right to privacy must be observed for private files, as must the protection of the secrecy of correspondence. Accordingly, the employer must avoid accessing private documents, files and

e-mails. However, a review of private documents, files and e-mails may be permissible in the event of particularly serious violations if the employer's interest in the review outweighs the employee's interest in safeguarding his right to privacy. Generally, employers should allow private use of electronic devices only if employees have previously consented to the terms of use (including searches in certain cases).

A search of the employee's workplace by the employer is, in principle, permissible. However, a search of personal items (eg, bags, clothes, personal mobile phone) is generally only permissible with the employee's consent. Similarly to the review of digital personal data, a search of personal items may be permitted, however, in the event of particularly serious violations if the employer's interest in the search outweighs the employee's right to privacy.

Last updated on 15/09/2022

Greece

Author: *Angeliki Tsatsi, Anna Pechlivanidi, Pinelopi Anyfanti, Katerina Basta*
at Karatzas & Partners

As a first step, the employer should ask for the employee’s permission to access their possessions and files. Employment contracts and internal labour regulations may include provisions regarding an employer’s access to employees’ documents created and kept for business purposes or related to business activity.

Last updated on 03/04/2023

Hong Kong

Author: *Wynne Mok, Jason Cheng, Audrey Li*
at Slaughter and May

As part of an investigation, an employer may search objects or files that are the company’s property (eg, electronic devices given by the employer for business purposes and emails or messages stored on the company’s server) without prior notice and the employee’s consent is not needed. The employer, however, has no right to search an employee’s possessions (eg, a private smartphone) without the employee’s consent.

To avoid arguments as to who a particular object belongs to, employers may specify in internal policies what is to be regarded as a corporate asset and could be subject to a search in a workplace investigation.

Concerning an employee’s possessions, even if he or she consents to a search, it is good practice for the employer to conduct the search in the presence of the employee or an independent third party who can act as a witness to the search. If the employer suspects that a criminal offence has been committed and that a search of the employee’s possessions would reveal evidence, the employer should consider reporting its suspicion to the police, as they have wider legal powers to search.[1]

---

[1] Usually upon execution of a warrant.

Last updated on 27/11/2023

India

Author: *Atul Gupta, Kanishka Maggon, Kopal Kumar*
at Trilegal

Yes, an employer can search its employees' official possessions and files as part of an investigation. It may be difficult, however, to seize personal assets or possessions of an employee (such as the individual's mobile phone or personal laptop).

Employers should expressly create policies that address key issues associated with employee surveillance, forensic searches and investigations, such as:

- whether or not the official assets and infrastructure of the company can be used for personal purposes by employees;
- the organisation's right to monitor, surveil or search any authorised or unauthorised use of its corporate assets; and
- that the employee should not have any expectation of privacy when using the companies' resources, etc.

Any forensic review of digital data must be carried out with due regard to Indian rules of evidence to avoid situations where such evidence becomes unreliable in a future legal claim or dispute.

Last updated on 15/09/2022

Ireland

Author: *Bláthnaid Evans, Mary Gavin*
at Ogier

The first consideration here is what constitutes "employees' possessions". More often than not, employees will be using employer property and there should be clear policies in place that specify company property.

The difficulty arises if an employee is using personal equipment such as a mobile phone for work purposes. While there may be specific applications dealing with work-related matters that are accessible by the employer remotely, some applications may be device-specific and that is where issues may arise. In such instances, it is not unreasonable to ask the employee to provide such information or consent to a search of their personal property. However, this is the exception rather than the rule and all other legitimate avenues of obtaining such information should be explored first. Further, such requests for information should not be a fishing expedition as an employee has a reasonable expectation of privacy at work, which must be balanced against the rights of the employer to run their business and protect the interests of their organisation.

A search of physical items such as a desk or drawers should only be conducted in exceptional circumstances, even where there is a clear, legitimate justification to search and the employee should be present at the search.

Last updated on 11/10/2023

Italy

Author: *Giovanni Muzina, Arianna Colombo*
at BonelliErede

In light of the legal and case-law principles as outlined above:

- see question 7 regarding employee "physical inspections and inspections on the employee's belongings";
- regarding "audiovisual equipment and other instruments from which the possibility of remote control of employees' activities also arises", article 4 of the Workers' Statute provides for:
    - the prohibition of the use of audiovisual equipment and instruments of "direct" remote control (ie, whose sole purpose is to verify the manner, quality and quantity of working performance (eg, a

camera installed in an office to film employees' working activities, without any other purpose));
    - the possibility of carrying out controls through audiovisual equipment and "indirect" remote instruments (ie, instruments that serve different needs (organisational, production, work safety or company assets' protection), but which indirectly monitor working activities (eg, a camera installed in a warehouse to prevent theft, but which indirectly monitors the activity of warehouse workers), which may only be installed with a trade union agreement (or National Labour Inspectorate authorisation);
    - the possibility of carrying out checks using working tools in the employee's possession (e.g., PCs, tablets, mobile phones, e-mail), which may be carried out even in the absence of any trade union agreement, provided that the employee is given adequate information on how to use the tools and how checks may be carried out on their use (according to privacy law strictly related to the employment relationship).

Furthermore, based on case law, the employer can carry out so-called defensive controls (ie, actions carried out in the absence of the guarantees provided for in article 4, to protect the company and its assets from any unlawful conduct by employees). These "defensive controls" can be carried out if:

- they are intended to determine unlawful behaviour by the employee (ie, not simply to verify his or her working performance);
- there is a "well-founded suspicion" that an offence has been committed;
- they take place after the conduct complained of has been committed; and
- adequate precautions are nevertheless put in place to guarantee a proper balancing between the need to protect company assets and safeguarding the dignity and privacy of the employee.

Last updated on 15/09/2022

Japan

Author: *Chisako Takaya*
at Mori Hamada & Matsumoto

Since inspections of personal belongings may potentially undermine employees' fundamental human rights, they would not become lawful simply because they are conducted under employment regulations.

Inspections of personal belongings must be conducted uniformly among employees in the workplace based on reasonable grounds, in a generally reasonable manner and to a generally reasonable degree, and based on the work rules, etc.

When inspections of personal belongings are conducted under employment regulations, etc, employees must agree to the inspection except in special circumstances, such as the method or degree of the inspection being unreasonable.

On the other hand, an investigation of information stored on a company network system may constitute an infringement of the right to privacy. If there is a provision in the employment regulations regarding the use of the internet and monitoring, it is possible to investigate under such a provision. A Japanese court case on the illegality of reading e-mails in the absence of a monitoring provision stated that private use of e-mails also carries a certain right to privacy, but also stated that "considering the fact that the system is maintained and managed by the company, the protection of the employee's privacy can only be expected within a reasonable range according to the specific circumstances of the system," and that the act of reading e-mails was not illegal because the extent of private use of e-mails was beyond the limit, which was outside the reasonable range of socially accepted ideas. The court also ruled that the monitoring of the employee's abusive private use of e-mail, which was discovered in the course of an investigation of slanderous e-mails within the company, was not illegal because even if the monitoring was conducted without notice, there was suspicion of a violation of the duty of devotion to duty and corporate order. The court also stated that the investigation was necessary and that the scope of the investigation did not exceed its limit.

Last updated on 15/09/2022

Netherlands

Author: *Barbara Kloppert, Mirjam Kerkhof, Roel de Jong*
at De Brauw Blackstone Westbroek

When conducting an internal investigation (which must have a legitimate purpose), the employer must act in accordance with the principles of proportionality and subsidiarity. In line with these principles, the means of collecting and processing personal data during an internal investigation as well as the data that is searched, collected or processed, should be adequate, relevant and not excessive given the purposes for which the data is being collected or subsequently processed. These principles can be complied with by, for example, using specific search terms when searching electronic data, limiting the investigation's scope (subject matter, period, geographic locations) and, in principle, excluding an employee's private data.

The employer is, in principle, allowed to access documents, emails and internet connection history saved on computers that were provided to the employees to perform their duties, provided the requirements of proportionality and subsidiarity are taken into account. In other words, reading the employee's emails or searching electronic devices provided by the employer must serve a legitimate purpose (e.g. tracing suspected irregularities or abuse) and the manner of review or collecting and processing the data contained in such emails should be in accordance with the principles of proportionality and subsidiarity.

The employer can ask the employee to hand over an employee's USB stick for an investigation. Depending on company policies and (individual or collective) employment agreements, an employee is, in principle, not obliged to comply with such a request. A refusal from an employee, when there is a strong indication that this USB stick contains information that is relevant to an investigation into possible irregularities, may be to the disadvantage of an employee, for example in a dismissal case.

The following factors, which derive from the Bărbulescu judgment of the European Court of Human Rights, are relevant to the question of whether an employee's e-mail or internet use can be monitored:

- whether the employee has been informed in advance of (the nature of) the possible monitoring of correspondence and other communications by the employer;
- the extent of the monitoring and the seriousness of the intrusion into the employee's privacy;
- whether the employer has put forward legitimate grounds for justifying the monitoring;
- whether a monitoring system using less intrusive methods and measures would have been possible;
- the consequences of the monitoring for the employee; and
- whether the employee has been afforded adequate safeguards, in particular in the case of intrusive forms of monitoring.

These requirements can sometimes create a barrier for employers, as seen in a ruling by the District Court Midden-Nederland (16 December 2021, ECLI:NL:RBMNE:2021:6071) in which the employer had used information obtained from the employee's e-mail as the basis for a request for termination of the employment contract. In the proceedings, the employee argued that his employer did not have the authority to search his e-mail.

According to the District Court, it was unclear whether the employer had complied with the requirements of Bărbulescu regarding searching the employee's e-mail. The regulations submitted by the employer only described the processing of data flows within the organisation in general. Therefore, the District Court found that the employer did not have a (sufficient) e-mail and internet protocol and the employee was not properly informed that his employer could monitor him. In addition, according to the District Court, it was unclear what exactly prompted the employer to search the employee's e-mail, as the employer did not provide any insight into the nature and content of the investigation. As a result, the District Court was unable to determine whether the employer had legitimate grounds to search the employee's e-mail. On this basis, the District Court disregarded the (possibly) illegally obtained evidence and ruled against the employer's termination request.

Last updated on 27/11/2023

Nigeria

Author: *Adekunle Obebe*
at Bloomfield LP

Yes, an employer can search the possessions or files of an employee as part of an investigation where the employee's contract or handbook authorises such a search and there is a reasonable suspicion of wrongdoing.

Last updated on 15/09/2022

Philippines

Author: *Rashel Ann C. Pomoy*
at Villaraza & Angangco

Subject to the employees' reasonable expectation of privacy, gathering physical evidence within the premises of the workplace and through company-issued property has been upheld to be legally permissible in pursuit of the employer's right to conduct work-related investigations. The search, however, should be limited to the alleged acts complained of and must not be used as a fishing expedition to find incriminating information about the erring employee.

Last updated on 26/01/2023

Poland

Author: *Wioleta Polak, Aleksandra Stępniewska, Julia Jewgraf*
at WKB Lawyers

It depends on whether the employer implemented rules of personal control at the workplace. If yes, such rules are applicable. If not, in our opinion if there is suspicion of a serious violation, it is possible to carry out an ad hoc inspection but its scope should be limited only to necessary activities and should not concern an employee's private files or correspondence, so as not to infringe on personal rights. If there is an ad hoc inspection, an employee should be informed in advance, and it should take place in the presence of the employee or employee's representative, observing the rules of fairness and equity.

Last updated on 20/04/2023

Portugal

Author: *André Pestana Nascimento*
at Uría Menéndez - Proença de Carvalho

The employer is allowed to search an employee's possessions or files, provided that they are work instruments or of a professional nature.

When performing these searches, employers should consider the specific provisions of the Data Protection Regulations as well as Resolution No. 1638/2013 of the Portuguese Data Protection Authority (CNPD), which contains rules on monitoring phone calls, e-mail and internet usage by employees. The CNPD understands

that for the employer to access the employees' professional data (e-mails, documents and other information stored on electronic devices), the latter should be present during the monitoring, to identify any information of a personal nature that should not be accessed by the employer (the employer must comply with these directions and should not access that email). In addition, review of the data should respect specific protocols to avoid potential access to personal data (eg, review of subject, recipients, data flow and type of files attached).

Body searches or the seizure of personal belongings or documents belonging to the employee are not permitted within the scope of a disciplinary procedure.

Last updated on 15/09/2022

Singapore

Author: *Jonathan Yuen, Doreen Chia, Tan Ting Ting*
at Rajah & Tann Singapore

The employer is not allowed to search employees' personal possessions or files as part of an investigation without the employee's consent. However, such consent may be explicitly provided for in the terms of employment (as may be contained in the employment contract, employee handbook or the employer's internal policies and procedures in dealing with the investigations, etc). The employer may, however, search the employees' company email accounts and files if these are stored on the company's internal systems or devices.

Last updated on 15/09/2022

South Korea

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

As discussed in question 7, it may be difficult for a company to search an employee's personal possessions. The company may search and gather electronic data stored in work laptops or company servers, subject to legal requirements and restrictions (eg, obtaining consent).

The PIPA provides specific guidance on the requirements for obtaining consent. Under the PIPA, to collect or use an individual's personal information, the information holder must be informed of and consent to:

- the purpose of the collection or use;
- the personal information that will be collected;
- the period of retention and use; and
- his or her right to refuse to provide consent and any disadvantages that may result from such refusal.

There are separate requirements for obtaining consent to provide an individual's personal information to a third party. Also, consent must be obtained separately for the collection, use or provision of sensitive or unique identification information.

Under limited circumstances, personal information may be collected, used, or provided to third parties without obtaining the consent of the information holder. For instance, a company may collect and use personal information without obtaining consent where obtaining the information is necessary to achieve the company's "legitimate interests", which clearly exceed the information holder's right to his or her personal information, and the collection and use are carried out within reasonable bounds. The term "legitimate interests" in this context is generally understood as a concept similar to "justifiable act" under the Criminal Code. The Korean Supreme Court has held that under exceptional circumstances such as the following, the company's collection and review of employee data may constitute a "justifiable act" under the Criminal Code:

1. the company had specific and reasonable suspicion that the employee had committed a crime and the company had an urgent need to verify the facts;
2. the scope of the company's review was limited to the suspected crime through the use of keywords, etc;
3. the employee had signed an agreement stating that he or she would not use work computers in an unauthorised manner and that all work products would belong to the company; and
4. the company's review uncovered materials that could be used to verify whether the employee committed the alleged crime.

Last updated on 15/09/2022

Spain

Author: *Sergio Ponce, Daniel Cerrutti*
at Uría Menéndez

Please see question 7.

Last updated on 15/09/2022

Sweden

Author: *Henric Diefke, Tobias Normann, Alexandra Baron*
at Mannheimer Swartling

An employer can search an employee's personal possessions (eg, handbag, pockets and locker) if the employer has a legitimate interest in a search. This could, for example, include a reasonable suspicion of theft of employer property. Furthermore, an employer may search, but not continually monitor, an employee's computer and email provided that it is in accordance with GDPR requirements. For the processing to be lawful under the GDPR, the employer has to establish a purpose and a legal basis for the processing of personal data. Furthermore, data subjects must have received information on the legal basis for and purpose of the processing of personal data beforehand. If the data subjects have not received such information, the employer's right to process their data is limited. However, if the employer has reasonable grounds to believe that trade secrets or similar has been copied and stolen, no such requirements would typically apply.

Investigations into an employee's possessions may, under certain circumstances, also be carried out by the Swedish authorities.

Last updated on 15/09/2022

Switzerland

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

The basic rule is that the employer may not search private data during internal investigations.

If there is a strong suspicion of criminal conduct on the part of the employee and a sufficiently strong justification exists, a search of private data may be justified.[1] The factual connection with the employment relationship is given, for example, in the case of a criminal act committed during working hours or using workplace infrastructure.[2]

[1] Claudia Fritsche, Interne Untersuchungen in der Schweiz: Ein Handbuch für regulierte Finanzinstitute und andere Unternehmen, Zürich/St. Gallen 2013, p. 168.

[2] Claudia Fritsche, Interne Untersuchungen in der Schweiz: Ein Handbuch für regulierte Finanzinstitute und andere Unternehmen, Zürich/St. Gallen 2013, p. 168 et seq.

Last updated on 15/09/2022

Thailand

Author: *Ratthai Kamolwarin, Norrapat Werajong*
at Chandler MHM

Electronic information created during employment would generally be owned by the employer and would be the employer's assets. If an employee is given a computer or laptop to use for work, the employer has the right to log into that device and take any data that is stored therein, provided that the data does not contain sensitive information of that employee and PDPA requirements are met.

To avoid any potential issues regarding physical data such as documents on the employee's desk, it is advisable to search those areas with the subject employee to show good faith. In practice, the employee normally agrees to search those areas with the employer, or allows the employer to search alone.

Last updated on 15/09/2022

Turkey

Author: *Elvan Aziz, Gülce Saydam Pehlivan, Emre Kotil, Osman Pepeoğlu*
at Paksoy

There is no explicit answer to this question. However, it is important to make a distinction between employees' possessions and files that are strictly personal and employees' possessions and files that are found on devices or files provided for company use. For the first category, the employer does not have the right to search employees' possessions and files. For the latter category though, justifications need to be established, by observing the requirements explained in question 7. Furthermore, the employers must also ensure that employees are fully and explicitly informed in advance of the monitoring operations, either through a provision included in the employment agreement, or in a separate notice or employee policy, the receipt of which should be duly acknowledged by the employee.

Last updated on 15/09/2022

United Kingdom

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

It may sometimes be difficult to draw a clear distinction between the property of the employer and employees' personal property, both physical and electronic, particularly where employees are increasingly working from home. Employers should ideally have a clear policy to delineate what is the employer's property.

Employees typically have a reasonable expectation of privacy at work, although how far this extends will depend on the circumstances of each case and the employer's policies.

When it comes to employees' personal possessions, a search should only be conducted in exceptional circumstances where there is a clear, legitimate justification. The employer should always consider whether it is possible to establish the relevant facts through the collection of other evidence. Even if the employee's contract specifies that it is permitted, employers would usually require explicit employee consent for the search to be lawful. The employee should be invited to be present during the search; if this is not feasible, another independent third party (such as a manager) should be present.

If the employee refuses to consent to a search of their personal possessions, their refusal should not be used to assume guilt; the investigator should explore why the employee has refused and seek to resolve their concerns if possible.

If the employer believes that a criminal offence has been committed it should consider involving the police, since they have wider powers to search individuals and their possessions.

Last updated on 15/09/2022

United States

Author: *Rachel G. Skaistis, Eric W. Hilfers, Jenny X. Zhang*
at Cravath, Swaine & Moore

As there is no unified data protection regime, privacy protections stem from a patchwork of federal and state privacy laws which impose limits on the extent to which an employer can collect information from its employees in connection with an internal investigation. Whether specific conduct violates an employee's rights is a very fact-specific inquiry requiring the application of relevant state laws and a regulatory regime.

In most circumstances, an employer is free to conduct searches of its workplace and computer systems in the course of investigating potential wrongdoing. Such searches are generally not protected by personal privacy laws because workspaces, computer systems and company-issued electronic devices are often considered company property. Many companies explicitly address this in written corporate policies and employment agreements. Employees who use their own electronic devices for work should be aware that work-related data stored on those devices is generally considered to belong to the employer (as a matter of best practice, employers should generally prohibit or at least advise employees against using personal devices for work and to maintain separate work devices, where possible).

These broad investigatory powers notwithstanding, the ability of an employer to conduct searches in furtherance of an internal investigation is not unlimited. For example, if an employer seeks to obtain or review work-related data from an employee's personal device, the employer must be careful to exclude any personal data. Certain states also prohibit an employer from requiring an employee to disclose passwords or other credentials to his or her personal email and social networking accounts, but permit an employer to require employees to share the content of personal online accounts as necessary during an interview while investigating employee misconduct.

Last updated on 15/09/2022

Vietnam

Author: *Stephen Le, Trang Le*
at Le & Tran Law Corporation

As part of an investigation, an employer may search the objects or files that are part of the company's property (eg, company or employers' laptops or phones for business purposes and emails or messages stored on the company's servers) without prior notice and without the need of the consent of the employee. However, the employer has no right to search an employee's personal possessions without consent.

To further avoid arguments or conflicts as to the right of ownership of a particular object or property, employers may specify in their internal policies, labour contracts, and handover documents what is to be regarded as the company's assets and subject to a search in a workplace investigation.

Last updated on 25/09/2023

Contributors

Australia

Joydeep Hor
Kirryn West James
Chris Oliver
People + Culture Strategies

Austria

Michaela Gerlach
Sonia Ben Brahim
GERLACH

Belgium

Nicolas Simon
Van Olmen & Wynant

Brazil

Patricia Barboza
Maury Lobo
CGM

China

Leo Yu
Yvonne Gao
Tracy Liu
Larry Lian
Jingtian & Gongcheng

Finland

Anu Waaralinna
Mari Mohsen
Roschier

France

Pascale Lagesse
Valentino Armillei
Bredin Prat

Germany

Hendrik Bockenheimer
Susanne Walzer
Musa Müjdeci
Hengeler Mueller

Greece

Angeliki Tsatsi
Anna Pechlivanidi
Pinelopi Anyfanti
Katerina Basta
Karatzas & Partners

Hong Kong

Wynne Mok
Jason Cheng
Audrey Li
Slaughter and May

India

Atul Gupta
Kanishka Maggon
Kopal Kumar
Trilegal

Ireland

Bláthnaid Evans
Mary Gavin
Ogier

Italy

Giovanni Muzina
Arianna Colombo
BonelliErede

Japan

Chisako Takaya
Mori Hamada & Matsumoto

Netherlands

Barbara Kloppert
Mirjam Kerkhof
Roel de Jong
De Brauw Blackstone Westbroek

Nigeria

Adekunle Obebe
Bloomfield LP

Philippines

Rashel Ann C. Pomoy
Villaraza & Angangco

Poland

Wioleta Polak
Aleksandra Stępniewska
Julia Jewgraf
WKB Lawyers

Portugal

André Pestana Nascimento
Uría Menéndez - Proença de Carvalho

Singapore

Jonathan Yuen
Doreen Chia
Tan Ting Ting
Rajah & Tann Singapore

South Korea

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

Spain

Sergio Ponce
Daniel Cerrutti
Uría Menéndez

Sweden

Henric Diefke
Tobias Normann
Alexandra Baron
Mannheimer Swartling

Switzerland

Laura Widmer
Sandra Schaffner
Bär & Karrer

Thailand

Ratthai Kamolwarin
Norrapat Werajong
Chandler MHM

Turkey

Elvan Aziz
Gülce Saydam Pehlivan
Emre Kotil
Osman Pepeoğlu
Paksoy

United Kingdom

Phil Linnard
Clare Fletcher
Slaughter and May

United States

Rachel G. Skaistis
Eric W. Hilfers
Jenny X. Zhang
Cravath, Swaine & Moore

Vietnam

Stephen Le
Trang Le
Le & Tran Law Corporation