Bloomberg BNA

Bloomberg Law®: Privacy & Data Security

Workplace Privacy Requirements: SWITZERLAND

Dr. Jürg Schneider and Dr. Monique Sturny, of Walder Wyss Ltd., Zurich, Switzerland, provided expert review of the Switzerland Workplace Privacy Requirements. [Last updated August 2016. – Ed.]

100. WORKPLACE PRIVACY—INTRODUCTION

The right to privacy is recognized as a fundamental right in the Federal Constitution of the Swiss Confederation.[1] Specifically, the Constitution states that "[e]very person has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications" (Constitution, art. 13, ¶ 1). Further, "[e]very person has the right to be protected against the misuse of their personal data" (Constitution, art. 13, ¶ 2).

Data privacy in Switzerland is governed by the Federal Act on Data Protection (FADP).[2] The FADP is supplemented by the Ordinance to the Federal Act on Data Protection (OFADP)[3] and by the Ordinance on Data Protection Certification (DPCO).[4] The FADP and the associated ordinances apply to the processing of personal data by private bodies and Swiss federal bodies. Under Swiss federal data protection law, protections exist for personal data, sensitive personal data, and personality profiles. Note that further data protection-related rules may be relevant in specific cases (such as, *e.g.*, banking secrecy provided in art. 47 of the Swiss Federal Banking Act[5]). Furthermore, cantonal data protection laws apply to any data processing by cantonal bodies. There are 26 cantons in Switzerland and hence 26 different cantonal regimes. Such cantonal data protection laws may have a broader scope of protection than the FADP (*e.g.*, the Act on Information and Data Protection of the Canton of Zurich [IDG][6] applies to "information" at large, IDG § 1, ¶ 1).

According to the FADP, "personal data" is all information relating to an identified or identifiable natural or legal person (FADP art. 3, ¶ a). Hence, unlike the data protection regulations of most other countries, the FADP applies not only to natural persons, but equally to legal entities. An increased level of protection applies to sensitive personal data and personality profiles. "Sensitive personal data" is data on (i) religious, ideological, political, or trade union-related views or activities; (ii) health, the intimate sphere, or racial origin; (iii) social security measures; and (iv) administrative or criminal proceedings and sanctions (FADP art. 3, ¶ c). A "personality profile" is a collection of data that permits an assessment of essential characteristics of the personality of a natural

[1] Federal Constitution of the Swiss Confederation of April 18, 1999, *unofficial English translation provided by the Swiss government at* https://www.admin.ch/opc/en/classified-compilation/19995395/201506140000/101.pdf.

[2] Federal Act of 19 June 1992 on Data Protection (FADP), *unofficial English translation provided by the Swiss government at* https://www.admin.ch/opc/en/classified-compilation/19920153/201401010000/235.1.pdf.

[3] Ordinance of 14 June 1993 to the Federal Act on Data Protection (OFADP), *unofficial English translation provided by the Swiss government at* https://www.admin.ch/opc/en/classified-compilation/19930159/201210160000/235.11.pdf.

[4] Ordinance of 28 September 2007 on Data Protection Certification (DPCO), *unofficial English translation provided by the Swiss government at* https://www.admin.ch/opc/en/classified-compilation/20071826/201004010000/235.13.pdf.

[5] Federal Banking Act of 8 November 1934, *available in German at* https://www.admin.ch/opc/de/classified-compilation/19340083/index.html).

[6] Act on Information and Data Protection of the Canton of Zurich (IDG) of 12 February 2007, *available in German at* http://www2.zhlex.zh.ch/appl/zhlex_r.nsf/0/9F174CBC94C4502BC12577E10046DD53/$file/170.4_12.2.07_71.pdf.

person (FADP art. 3, ¶ d). Personality profiles are protected to the same extent as sensitive personal data.

With respect to the processing of personal data of employees, art.328*b* of the Swiss Federal Code of Obligations (CO)[7] applies in addition to the FADP. CO art.328*b* provides that an employer may handle employee data only to the extent it concerns the employee's suitability for his job or is necessary for the performance of the employment contract. In addition, art. 26 of Ordinance 3 to the Employment Act[8] prohibits the use of systems that monitor the behavior of employees at the workplace. However, to the extent monitoring systems are necessary for other reasons (such as quality control, security purposes, technical reasons, etc.), they must be designed so as not to impair the health or movement of employees. If monitoring is required for legitimate reasons, it must at all times remain proportionate (*i.e.*, limited to the extent absolutely required), and the employees must be informed in advance about the use of such monitoring systems. Permanent monitoring is generally not permitted.

Data protection compliance by private and federal bodies is supervised by the Swiss Federal Data Protection and Information Commissioner (Commissioner). The Commissioner supervises federal and private bodies, advises and comments on the legal provisions governing data protection, and assists federal and cantonal authorities in the field of data protection. In addition, the Commissioner informs the public about his findings and recommendations, and maintains and publishes the register of data files. The Commissioner has issued a specific Guide on the Processing of Personal Data in the Workspace.[9] Although the guide is not legally binding, it sets *de facto* standards.

300. Background Checks

300.10. Laws and Regulations Governing Background Checks

Key laws and regulations include, *inter alia*:

- Federal Act on Data Protection (FADP)
- Ordinance to the Federal Act on Data Protection (OFADP)
- Ordinance on Data Protection Certification (DPCO)
- Article 328*b* of the Swiss Code of Obligation (CO)
- Article 26 of Ordinance 3 to the Employment Act
- Guide on the Processing of Personal Data at the Workplace
- Guide on Internet and Email Surveillance at the Workplace

In contrast to the FADP, the CO, and the Ordinances mentioned above, the two guides mentioned are not legally binding. However, they set *de facto* standards that are relevant in practice. The Commissioner has published further information and documents relating to data protection at the workplace on its website.

300.20. Information Collection

300.20.10. Information Collection — In General

General data protection principles

The FADP outlines general data protection principles (FADP art. 4, art. 5, ¶ 1 and art. 7, ¶ 1). These principles state that:

- personal data must be processed lawfully;
- the processing must be carried out in good faith and be proportionate;
- personal data may only be processed for the purpose indicated at the time of collection;
- the collection of personal data and in particular the purpose of data collection must be evident to the data subject concerned (so-called principle of transparency);
- if the legality of data processing is based on the consent of the data subject concerned, such consent must be given voluntarily and upon provision of adequate information. If such processing relates to sensitive personal data or personality profiles, such consent must be given expressly (FADP art. 4, ¶ 5). Consent is not required in all instances. However, consent may be a possible form of justification for data processing that would otherwise constitute a violation of the personality rights of the data subject concerned (*e.g.*, in a case of data processing that would oth-

[7] Federal Act on the Amendment of the Swiss Civil Code, Part Five: The Code of Obligations of 30 March 1911, *unofficial English translation provided by the Swiss government at* https://www.admin.ch/opc/en/classified-compilation/19110009/index.html#a328b.

[8] Ordinance 3 to the Employment Act of 18 August 1993, art. 26, *available in German at* https://www.admin.ch/opc/de/classified-compilation/19930254/index.html#a26.

[9] Leitfaden über die Bearbeitung von Personendaten im Arbeitsbereich (Guidance on the Processing of Personal Data in the Workplace), *available in German at* http://www.edoeb.admin.ch/datenschutz/00628/00629/00633/index.html?lang=de.

erwise be considered disproportionate). In the area of processing of employee data, the limits of CO art.328*b* need to be respected in each case. It is unclear if and to what extent employees may validly consent to processing of their personal data that goes beyond what is covered by CO art.328*b*. In addition, consent is only valid if given freely, which may not always be the case in an employment context. According to the opinion of the Commissioner, employee consent as a form of justification must be examined very critically, as the voluntariness of employee consent is often doubtful due to the relationship of subordination between the employer and the employee (*cf. e.g.*, Guide on Internet and Email Surveillance at the Workplace § 3.1)[10];
- the data handler must ensure that the data is accurate and kept up to date; and
- personal data must be protected against unauthorized processing through adequate technical and organizational security measures. If the controller of the data file engages a third party as a data processor, the controller must in particular ensure that such third party processes the personal data according to the instructions of the controller and that such third party implements adequate security measures.

Registration of data files

Controllers of data files who regularly process sensitive personal data or personality profiles, or who regularly disclose personal data to third parties (including affiliates), must declare their data files to the Commissioner for registration before they start processing such data (FADP art. 11*a*). The Commissioner maintains a register of such data files that is accessible online. Several exceptions apply to the duty to register data files. *Inter alia*, the registration requirement does not apply if the controller of the data file has a legal obligation to process the data in question, if the Federal Council has exempted the processing from the registration requirement because it does not prejudice the rights of the data subjects, or if the controller of data files has designated a data protection officer who independently monitors internal compliance with data protection regulations and maintains a list of the data files (FADP art. 11*a*, ¶ 5). A willful breach of the obligation to declare data files to the Commissioner for registration is criminally sanctioned with a fine of up to CHF 10,000 (FADP art. 34, ¶ 2, a).

Enhanced protection level for sensitive personal data and personality profiles

In addition to the duty to declare data files to the Commissioner for registration in case of regular processing of sensitive personal data or personality profiles (see above), further specific rules ensuring an enhanced protection level for these two types of data need to be adhered to:

- Sensitive personal data and personality profiles may not be disclosed to third parties for such third parties' own purposes without justification (FADP art. 12, ¶ 2, c). Possible forms of justification are consent, an overriding private or public interest, or a justification provided by law (FADP art. 13, ¶ 1). If such justification is based on the consent of the data subject, such consent is only valid if given expressly (FADP art. 4, ¶ 5).
- The controller of the data file is obliged to inform the data subject of the collection of sensitive personal data and/or personality profiles (FADP art. 14, ¶ 1). This duty to inform also applies where the data is collected from third parties (FADP art. 14, ¶ 1). The data subject must be informed of at least: (i) the identity of the controller of the data file, (ii) the purpose of the processing, and (iii) the categories of data recipients if a disclosure of data is planned (FADP art. 14, ¶ 2). Private persons are, on complaint, liable to a fine of up to CHF 10,000 if they willfully fail to (i) inform the data subject in accordance with FADP art. 14, ¶ 1, or (ii) provide information required under FADP art. 24, ¶ 2 (FADP art. 34, ¶ 1, b).

300.20.20. Information Collection Restrictions

300.20.20.10. Financial Information

There are no provisions in the FADP or its associated ordinances that specifically address the collection of financial information from employee candidates. Under the FADP, personal data is defined as all information relating to an identified or identifiable natural person or legal entity. Under this broad definition, financial information qualifies as personal data under the FADP. Hence, the FADP and in particular the general data protection principles need to be observed (see Section 300.20.10, above).

Furthermore, the limits of CO art.328*b* need to be respected, *i.e.*, the employer may handle data concerning an employee only to the extent such data con-

[10] Leitfaden Internet- und E-Mailüberwachung am Arbeitsplatz (Privatwirtschaft) (Guidelines Internet and Email Surveillance in the Workplace [Private Sector]), *available in German at* http://www.edoeb.admin.ch/datenschutz/00763/00983/00988/index.html?lang=de.

cerns the employee's suitability for his job or is necessary for the performance of the employment contract. Accordingly, the Commissioner's Guide on the Processing of Personal Data at the Workplace mentions that employers may inquire about an applicant's income or possible debt only if disclosure of such information is required for the job (see Guide § 3.1.2).

300.20.20.20. Criminal History

The Commissioner's Guide on the Processing of Personal Data at the Workplace mentions that employers may inquire about an applicant's criminal history only if such information is relevant to the position. For example, an employer seeking to fill a position for a cashier may ask an applicant if he has been convicted of embezzlement (see Guide § 3.1.2). However, general questions on criminal convictions are prohibited.

Information relating to the criminal history of a job applicant or employee qualifies as sensitive personal data (FADP art. 3, ¶ c). Therefore, unless the employer has appointed an internal data protection officer, employee data files containing information about the criminal history of a job applicant or employee must be declared to the Commissioner for registration. However, it can reasonably be argued that if the information on criminal history is relevant for the position of the employee, the employer may have a legal obligation to process such information and, thus, is exempt from the duty to declare such data files to the Commissioner for registration (see "*Registration of data files"* under Section 300.20.10, above). Furthermore, as such data qualifies as sensitive personal data, it is subject to an enhanced level of protection (see "*Enhanced protection level for sensitive personal data and personality profiles*" under Section 300.20.10, above).

300.20.20.30. Driving Records

There are no specific driving records in Switzerland. Only very serious road traffic offenses are shown in the criminal record extract for private persons. Hence, the same principles as for the processing of data relating to the criminal history of a job applicant apply (see Section 300.20.20.20, above). In particular, the employer may only inquire about an applicant's road traffic offenses if it is relevant to the position (*e.g.*, taxi driver or truck driver).

300.20.20.40. Work History and Educational Background

There are no provisions in the FADP or its associated ordinances that specifically address the collection of information concerning an employee candidate's work history or educational background. Under the FADP, personal data is defined as all information relating to an identified or identifiable person. Under this broad definition, information pertaining to work history and educational background for employee candidates qualifies as personal data according to the FADP. Hence, the FADP and in particular the general data protection principles must be observed (see "*General data protection principles*" under Section 300.20.10, above). In addition, the limits of CO art.328*b* need to be respected, *i.e.*, the employer may handle data concerning an employee's work history and educational background only to the extent such data concerns the employee's suitability for his job or is necessary for the performance of the employment contract.

300.20.20.50. References

The Commissioner's guide on Reference Information in the Application Process[11] indicates that references assess essential traits of the personality of an applicant and are therefore categorized as personality profiles under the FADP. Personality profiles are granted an enhanced level of protection similar to sensitive personal data (see "*Enhanced protection level for sensitive personal data and personality profiles*" under Section 300.20.10, above).

References must only be obtained with the prior consent of the job applicant. Such consent needs to be given expressly (FADP art. 4, ¶ 5). The guide states that when a candidate has merely listed a former employer in his job application, this does not qualify as consent. However, if the past employer is specifically listed on an application under the title "References," this would qualify as consent and approval for obtaining references.

As already mentioned, references pertaining to a job applicant or employee qualify as sensitive personal data (FADP art. 3 ¶ c). Therefore, unless the employer has appointed an internal data protection officer, employee data files containing job applicant or employee references of former employers must be

[11] Referenzauskünfte im Bewerbungsprozess (Reference Information in the Application Process), *available in German at* http://www.edoeb.admin.ch/dokumentation/00153/01251/01271/index.html?lang=de. The guide is not legally binding, but establishes *de facto* standards.

declared to the Commissioner for registration. However, it can reasonably be argued that the employer has a legal obligation to process such information as part of his duty of care and duty to provide references according to CO art.330*a*, and is, thus, exempt from the duty to declare such data files to the Commissioner for registration (see "*Registration of data files"* under Section 300.20.10, above). Furthermore, as such data qualifies as sensitive personal data, it is subject to an enhanced level of protection (see "*Enhanced protection level for sensitive personal data and personality profiles*" under Section 300.20.10, above).

300.30. Notice of Information Collection

The controller of the data file must inform the data subject (*i.e.*, the employee or job applicant) of any collection of personal data or other data processing that is not apparent from the circumstances. Enhanced information duties apply to the processing of sensitive personal data and personality profiles (such as criminal records and/or references). The controller of the data file is obliged to inform the data subject of the collection of sensitive personal data and/or personality profiles. This duty to inform also applies where the data is collected from third parties (FADP art. 14, ¶ 1). At a minimum, the data subject must be informed of: (i) the identity of the controller of the data file, (ii) the purpose of the processing, and (iii) the categories of data recipients if a disclosure of data is planned (FADP art. 14).

The controller of the data file must inform the data subject (*i.e.*, the employee or job applicant) of any collection of personal data or other data processing that is not apparent from the circumstances (see "*General data protection principles*" under Section 300.20.10, above, in particular, the principle of transparency).

Enhanced information duties apply to the processing of sensitive personal data and personality profiles (such as criminal records and/or references). The controller of the data file is obliged to inform the data subject of the collection of sensitive personal data and/or personality profiles (FADP art. 14, ¶ 1). This duty to provide information also applies where the data is collected from third parties (FADP art. 14, ¶ 1). At a minimum, the data subject must be informed of: (i) the identity of the controller of the data file, (ii) the purpose of the processing, and (iii) the categories of data recipients if a disclosure of data is planned (FADP art. 14, ¶ 2). Private persons are, on complaint, liable to a fine of up to CHF 10,000 if they willfully fail (i) to inform the data subject in accordance with FADP art. 14, ¶ 1, or (ii) to provide information required under FADP 24, ¶ 2 (FADP art. 34, ¶ 1, b).

The aforementioned information can be provided in the employment contract or, as it is often done in practice, in Employee Regulations or specific Employee Personal Data Processing Notices.

300.40. Access to, and Correction of, Information Collected

Any data subject may request that incorrect data be corrected (FADP art. 5, ¶ 2). Any person may request information from the controller of a data file as to whether data concerning him is being processed (FADP art. 8). The request must be in writing and be accompanied with proof of identity (OFADP art. 1, ¶ 1). The controller of a data file may refuse, restrict, or defer the provision of information where his own overriding interests so require and he does not disclose the personal data to third parties (FADP art. 9, ¶ 1). The controller of the data file must indicate the reason why he has refused, restricted, or deferred access to information (FADP art. 9, ¶ 5). With the consent of the controller of the data file or at his suggestion, the data subject may inspect his data on site. The information may also be provided verbally if the data subject has consented and has been identified by the controller of the data file (OFADP art. 1, ¶ 3). The information or a decision not to provide the information must be given within 30 days of receipt of the request (OFADP art. 1, ¶ 4). Private persons are, on complaint, liable to a fine of up to CHF 10,000 if they breach their obligations under FADP art. 8 - 10 by willfully providing false or incomplete information (FADP art. 34, ¶ 1, a).

300.50. Employment Verification Requests

There are no provisions in the FADP or in its associated ordinances that specifically address employment verification requests. Under the FADP, personal data is defined as all information relating to an identified or identifiable natural person or legal entity. Under this broad definition, employment verification requests would qualify as processing of personal data according to the FADP. Hence, the FADP and in particular the general data protection principles must be observed (see "*General data protection principles*" under Section 300.20.10, above).

500. Health Information, Medical Examinations, and Drug & Alcohol Testing

500.10. Health Information — In General

Under the FADP, health information is classified as sensitive personal data (FADP art. 3, ¶ c). Therefore, unless the employer has appointed an internal

data protection officer, employee data files containing health information may need to be declared to the Commissioner for registration. However, oftentimes the employer may have a legal obligation to process such information (*e.g.*, for insurance purposes) and is, thus, exempt from the duty to declare such data files to the Commissioner for registration (see "*Registration of data files"* under Section 300.20.10, above). Note that sensitive personal data is subject to an enhanced level of protection (see "*Enhanced protection level for sensitive personal data and personality profiles*" under Section 300.20.10, above).

500.20. Pre-Employment Health Questions

Neither the FADP nor the OFADP contains any provisions expressly governing the collection and processing of information for pre-employment health questions. The Commissioner has issued guidance on pre-employment health questions in its Guide on the Processing of Personal Data at the Workplace (§ 3.1.5) and also in its activity report 22 (2014/2015) with respect to "Health Questionnaires for Job Applicants." The Commissioner states that personal data about employees may only be procured, stored, or otherwise processed if such data relates to the suitability of the employment or is required to perform the employment contract. In addition, as information related to health history is classified as sensitive personal information under the FADP, such information is subject to greater protections. The employer may not enquire about job applicants' health conditions. However, the employer may ask job applicants to have medical checks conducted by a physician. Physicians are bound by professional confidentiality and may only inform the employer about the suitability of a job applicant for a certain position, but they may not communicate any diagnosis to the employer.

500.30. Medical Examinations

Neither the FADP nor the OFADP contains a provision expressly governing the collection and processing of information pursuant to a medical examination. As information related to medical examinations is classified as sensitive personal information under the FADP, such information is subject to an enhanced protection level (see "*Enhanced protection level for sensitive personal data and personality profiles*," under Section 300.20.10, above).

The Commissioner's Guide on the Processing of Personal Data at the Workplace indicates that employers may not inquire about the health of a job applicant, but they may consider a physician's assessment in order to evaluate a job applicant's suitability for the job. If a medical examination is required, the physician may disclose an applicant's physical suitability to perform the job, but the physician may not communicate any diagnosis to the employer (see Guide § 3.1.5).

500.40. Drug and Alcohol Testing

Neither the FADP nor the OFADP contains a provision expressly governing the collection and processing of employee information through drug and alcohol testing. As information related to drug and alcohol testing is classified as sensitive personal information under the FADP, such information is subject to an enhanced protection level (see "*Enhanced protection level for sensitive personal data and personality profiles*" under Section 300.20.10, above).

The Commissioner's Guide on the Processing of Personal Data at the Workplace indicates that a drug test with respect to apprentices ("Lehrlinge") in particular is permissible only if security interests outweigh the infringement of the apprentice's privacy rights and only if the apprentice has voluntarily and expressly consented. The apprentice must be clearly informed in advance about the purpose and consequences of any such test. The test must be conducted by a physician, and the employer may only be informed about the suitability of the apprentice for the position in question. The employer may not be provided with information about a possible drug use (see Guide § 3.1.7). In our view, there are strong arguments to hold that the aforementioned restrictions apply by analogy to job applicants as well as to regular employees.

500.50. Genetic Data

Neither the FADP nor the OFADP contains a provision expressly governing the collection and processing of genetic data. As genetic data is classified as sensitive personal information under the FADP, such information is subject to an enhanced protection level (see "*Enhanced protection level for sensitive personal data and personality profiles*" under Section 300.20.10, above).

The Commissioner's Guide on the Processing of Personal Data at the Workplace generally prohibits genetic testing of job applicants, but permits an exception where test results could determine unequivocally that a job applicant would put third parties at risk, and where the applicant has expressly consented to such test. Test results may only be communicated to the job applicant (see Guide § 3.1.6).

700. EMPLOYEE MONITORING AND SURVEILLANCE

700.10. Employee Monitoring and Surveillance — In General

The FADP and the OFADP do not specifically address the monitoring or surveillance of employees. However, the Commissioner has issued publications addressing certain areas of employee surveillance, including a Guide on Internet and Email Surveillance at the Workplace,[12] as well as guidelines on Bring Your Own Device (BYOD),[13] Mail and Electronic Mail,[14] and Questions from the Public on Workplace Surveillance.[15]

The Guide on Internet and Email Surveillance at the Workplace notes that log file data, *i.e.*, the digital trail left by computer users, constitutes personal data under the FADP. Hence, processing of such data is subject to the FADP's and the associated ordinances' provisions (see Guide § 2).

The Commissioner's guidance on Bring Your Own Device (BYOD) addresses employees' use of their own mobile devices at work. The use of personal devices elicits complex issues for an employer because oftentimes there is not a clear separation between personal information and business activities. The Commissioner recommends measures employers should implement in order to reduce privacy risks in a BYOD work environment. These include:

- establishing a clear policy in the form of special written instructions, stating what is allowed and what is not;
- maintaining the separation of business and personal data (technically and logically);
- employing measures (through encryption and passwords) to ensure data security;
- clearly delineating where business data is stored (on a local server if possible);
- designating a person responsible for approving employees' devices; and
- establishing regulations addressing access to the device by the employer.

As alternatives to BYOD, the Commissioner suggests four options: (i) Corporate Owned Personally Enabled (COPE) devices, where the employer selects preferred devices, buys them, yet allows employees limited, personal use; (ii) Choose Your Own Device (CYOD), in which the employee benefits from a supported device purchase, but the employer determines the configuration of the device and prohibits changes by employees; (iii) Bring Your Own Connection (BYOC), where a private cell phone is used as a hotspot; and (iv) Bring Your Own Software (BYOS), where portable applications are restricted to company-wide uniform rules.

As for workplace surveillance in general, the Commissioner advises employers to maintain transparency and clear communication. Employers must provide their employees with precise information about how the surveillance is being carried out, what is being evaluated, and what its purpose is. Regulations governing use and supervision should make it explicitly clear to employees that data concerning them will be processed. Employees must also be told clearly what e-mail, Internet, and other IT resources may and may not be used for. The aforementioned information is generally provided in the form of one or more detailed written policies (such as a combined acceptable use and monitoring use policy). See also Questions from the Public on Workplace Surveillance.

700.20. Electronic Communications

There are no provisions in the FADP or its associated ordinances that specifically address the monitoring or surveillance of an employee through electronic communications. However, the Commissioner has issued guidance relating to use and handling of Mail and Electronic Mail at the workplace, clarifying that an employer may not read the contents of marked or recognizable private e-mails, even if the private use of e-mail is prohibited by company rules. In addition, according to the Commissioner, the systematic monitoring of e-mails by spy programs (such as content scanners) is generally not permitted. However, the Commissioner recognizes that there may be specific areas in the private sectors (*e.g.*, banks) where a systematic surveillance and analysis of e-mails exchanged may be necessary in order to meet compliance requirements (Guide on Internet and Email Surveillance at the Workplace, § 4). This, however,

[12] Leitfaden Internet- und E-Mailüberwachung am Arbeitsplatz (Privatwirtschaft) (Guidelines Internet and Email Surveillance in the Workplace [Private Sector]), *available in German at* http://www.edoeb.admin.ch/datenschutz/00763/00983/00988/index.html?lang=de.

[13] Bring Your Own Device (BYOD), *available in German at* http://www.edoeb.admin.ch/datenschutz/00763/01249/index.html?lang=de.

[14] Brief- und elektronische Post (Mail and Electronic Mail), *available in German at* http://www.edoeb.admin.ch/datenschutz/00763/00807/00827/index.html?lang=de.

[15] Questions from the Public on Workplace Surveillance, *available in English at* http://www.edoeb.admin.ch/dokumentation/00153/00154/00165/index.html?lang=en.

needs to be checked in advance on a case-by-case basis and depends on the type of monitoring put in place.

700.30. Internet

There are no provisions in the FADP or its associated ordinances that specifically address the monitoring or surveillance of an employee through the Internet, but the Commissioner has issued a Guide on Internet and Email Surveillance at the Workplace, which specifies that log file data, *i.e.*, the digital trail left by computer users, constitutes personal data. Thus, processing of such data is subject to the FADP's and the associated ordinances' provisions (Guide § 2). Moreover, the use of keyloggers and monitoring programs that detect every activity of the employee on the computer are in general prohibited by article 26 of Ordinance 3 to the Employment Act (see Guide § 4).

700.40. Video Monitoring

While the FADP and the OFADP do not address video monitoring of employees, the Commissioner has issued Explanations on the Video Surveillance at the Workplace.[16] The instructions of the Commissioner regarding Video Surveillance by Private Individuals[17] and Video Surveillance of Public Places by Private Individuals[18] are also relevant in this context.

According to the Commissioner's Explanations on the Video Surveillance at the Workplace and instructions regarding Video Surveillance by Private Individuals, surveillance systems (such as video monitoring) that seek only to monitor the behavior of employees may not be used. However, if surveillance systems are necessary for other purposes (*e.g.*, security reasons, quality control), they must be implemented in a way that does not impair the health and liberty of the employee. If monitoring is required for legitimate reasons, it must at all times remain proportionate (*i.e.*, limited to the extent absolutely required), and employees must be informed in advance about the use of the monitoring system. Permanent monitoring is generally not permitted. The general limitations (in particular, CO art.328*b*, art. 26 of the Ordinance 3 to the Employment Act and FADP art. 13, see above for more details) must be respected. Surveillance is permitted only if an infringement of the personal privacy of the employee is justified (i) by consent (*n.b.*, employees may consent only within the limits set forth by CO art.328*b*); (ii) by an overriding public or private interest in the surveillance; or (iii) by law. In addition, the principles of proportionality and transparency must be respected. Any permissible surveillance must be restricted to the premises at hand and not a neighboring property. In addition, a clearly visible notice about the surveillance system must be set up. If recorded images are being stored, notice must also be given of who can be contacted for further information if this is not obvious from the circumstances.

With respect to the operation of a CCTV system, the Commissioner's guidance regarding Video Surveillance by Private Individuals provides that: (i) the data may only be used to protect persons and property, and not for any other purposes; (ii) appropriate technical and organizational measures must be put in place in order to protect the video images from being processed by unauthorized persons; (iii) access to both live and, if relevant, stored video images must be restricted to as few people as possible; (iv) the personal data recorded may not be disclosed unless the data handler is required to disclose the images to law enforcement authorities in order to assist in criminal proceedings, or in cases provided for or permitted by law (*e.g.*, binding and enforceable court order); (v) the images recorded must be deleted as soon as possible (*e.g.*, a retention period of 24 hours would normally seem sufficient if the images are taken in order to detect damage to property or personal injuries, as such incidents are normally reported within a few hours at a maximum; longer retention periods are permissible if justified on objective and important grounds, such as in case of absence of the property owner over public holidays); and (vi) the persons in charge of the video surveillance must provide information about the video surveillance to anyone coming within the range of the cameras.

The Commissioner's guidance regarding Video Surveillance of Public Places by Private Individuals states that protecting an individual's own security is not a legitimate reason for a private individual to monitor a public area. As a rule, private CCTV systems in public areas are generally regarded as an excessive and unlawful measure, and their installation is prohibited. There are, however, two possible exceptions to this rule. First, when a private individual conducts legitimate video surveillance of his private property (*i.e.*, in line with the conditions outlined

[16] Erläuterungen zur Videoüberwachung am Arbeitsplatz (Explanations on Video Surveillance at the Workplace), *available in German at* http://www.edoeb.admin.ch/datenschutz/00763/00983/00996/index.html?lang=de.

[17] Video Surveillance by Private Individuals, *available in English at* http://www.edoeb.admin.ch/datenschutz/00628/00653/00654/index.html?lang=en.

[18] Video Surveillance of Public Places by Private Individuals, *available in English at* http://www.edoeb.admin.ch/datenschutz/00625/00729/00738/index.html?lang=en.

above), it may in some cases be inevitable that images of public areas are also being recorded. Such surveillance is allowed if the extent of the intrusion is negligible and the surveillance of the private property would otherwise be impossible. Second, surveillance is allowable when a private individual wants to monitor a public area for security reasons and obtains permission of the competent authority (*i.e.*, the competent cantonal authority in case of video surveillance of public areas). When using CCTV systems with the permission of the competent cantonal authorities, the FADP nevertheless applies, and the general data protection principles must be observed (see Section 300.20.10, "*General data protection principles*", above).

It must further be noted that, according to art. 179quater of the Swiss Criminal Code (SCC),[19] a person who, without consent, observes with a recording device, or records with an image-carrying device, information from the secret domain of another person or information that is not automatically accessible from the private domain of another person is, on complaint, criminally liable to a custodial sentence not exceeding three years or to a monetary penalty of up to CHF 1,080,000.

700.50. Location Monitoring

The Commissioner has issued guidance entitled The Commercial Application of Personal Tracking Systems.[20] While the guidance principally addresses location monitoring of customers, it states unequivocally that tracking systems may not be used under any circumstances solely to monitor employee behavior. Doing so would be unlawful and could not be justified even if the employee had given consent in this respect. This is in line with the statements of the Swiss Federal Supreme Court in its decision dated July 13, 2004 (BGE 130 II 425), regarding the legitimacy of using GPS tracking systems in company vehicles.

While location monitoring may not be used for the sole purpose of monitoring the behavior of the employee, location monitoring may be lawful in exceptional cases if it is required for other reasons, such as for health and safety purposes, for quality controls, or as a means of evidence. However, the general data protection principles, in particular the principles of proportionality and transparency, must be observed at all times (see "*General data protection principles"* under Section 300.20.10, above). Specifically with respect to the principle of proportionality, the Supreme Court points out that there must be no less intrusive means available for reaching the intended legitimate purpose (*e.g.*, health, safety, evidence gathering, quality control) and that the tracking must be limited to the absolute minimum required for achieving the intended purpose. In addition, the interest of using location monitoring must outweigh the personality rights of the employees concerned in the specific case at hand. Relevant criteria for assessing proportionality are, *inter alia*, (i) whether the location monitoring relates only to work-related use of company vehicles (monitoring of private use would generally not be justified); (ii) whether there is only a time-shifted monitoring, and real-time monitoring is made technically impossible (real-time monitoring would in most cases be disproportionate); (iii) whether monitoring is only sporadic (*e.g.* , three or four hours a day) and not permanent (constant monitoring would be disproportionate); and (iv) whether the monitoring relates to an object (*e.g.*, car) and not to a person.

700.60. Telephone Use

There are no provisions in the FADP or its associated ordinances that specifically address the monitoring or surveillance of an employee's telephone use. However, the Commissioner's Guide on the Processing of Personal Data at the Workplace provides that employers may record numbers dialed at the workplace for professional purposes under the condition that (i) such recording is made for professional reasons (*e.g.*, in order to be able to charge calls to customers), and (ii) the employees concerned have been informed accordingly (Guide § 4.3.1).

The content of telephone conversations may be listened to and/or recorded only for performance assessment, *e.g.*, in the case of telephone sales or for training purposes, or in order to preserve evidence. The persons (the employee and any other participants to the call) whose voices are being recorded or listened to must be informed clearly and in advance about such surveillance (*e.g.*, to employees through an acoustic signal before each conversation or through a notice on the intranet of the employer; Guide § 4.3.2). To other participants to the call, notice must be given verbally in advance (*i.e.*, before the recording starts).

Any workplace prohibition on the personal use of telephones must be enforced by means other than employee monitoring, and, in any case, employees must

[19] Swiss Criminal Code of 21 December 1937, art. 179quater, *unofficial English translation provided by the Swiss government at* https://www.admin.ch/opc/en/classified-compilation/19370083/index.html#a179quater.

[20] The Commercial Application of Personal Tracking Systems, *available in English at* http://www.edoeb.admin.ch/dokumentation/00153/01174/01176/index.html?lang=en

be permitted to make calls from unmonitored phone lines in emergencies and during breaks (Guide § 4.3.3).

It must further be noted that, according to SCC art. 179bis, any person who, by using a listening device and without the permission of all those participating, listens in on a private conversation between other persons, or records such a conversation on a recording device, is, on complaint, and unless justified by a valid and recognized reason, criminally liable to a custodial sentence not exceeding three years or to a monetary penalty of up to CHF 1,080,000. Similarly, any person who, as participant in a private conversation, records the conversation on a recording device without the permission of the other participant, is, on complaint, and unless justified by a valid and recognized reason, liable to a custodial sentence not exceeding one year or to a monetary penalty of up to CHF 1,080,000 (SCC art. 179ter).

700.70. Searches and Inspections

There are no provisions in the FADP or its associated ordinances that specifically address searches or inspections of an employee. However, the general data protection principles (see "*General data protection principles*" under Section 300.20.10, above) must be observed. Prior to any monitoring or search of electronic devices such as computers, cell phones, etc., the employer is strongly advised to issue a detailed, written monitoring and acceptable use policy setting out the purposes for which employees may use a specific work tool (such as telephone, e-mail, etc.) and the limitations that apply. A search or monitoring without such a policy in place is in most cases illegal, unless there is a clear suspicion of a contractual breach or illegal behavior.

Inspections relating to the health of the employee constitute a severe infringement of the employee's personality rights. According to the Guide on the Processing of Personal Data at the Workplace (§ 3.1.5), the employer may not ask the employee or job applicant questions about his medical condition. However, the employer may ask an employee or job applicant to have medical checks conducted by a physician. Physicians are bound by professional confidentiality and may only inform the employer about the suitability of an employee or job applicant for a certain position; they may not communicate any diagnosis to the employer.

700.80. Biometrics

The Commissioner has published information on biometrics in "Some data protection considerations with regard to the use of biometric data in the private sector."[21] The guide provides an extensive list of principles that should be followed in order to guarantee data protection in connection with the use of biometric data. Specifically, the principles that should apply to the use of biometric systems in the private sector include, *inter alia*:

- biometrics should be used only when the intended objective cannot be achieved by less invasive methods;
- biometrics may be used for data protection and data security (see, however, below, certain restrictions on the use of biometric data with respect to work-related recording of time-keeping and access control);
- data subjects must be given clear notice and must be included in data processing procedures;
- biometric data must be collected directly from the data subject, or at least with his knowledge; and
- all necessary steps should be taken to avoid the use of biometric information as a universal user ID.

In addition, the Commissioner has issued guidance on the use of biometric data with respect to work related recording of time-keeping and access control,[22] a detailed guide on biometric recognition systems,[23] and additional information on data storage relating to biometric verification systems.[24]

According to the guidance on the use of biometric data with respect to work-related recording of time-keeping and access control, the Commissioner is of the opinion that the use of biometric recognition systems at the workplace is problematic, as such use constitutes a breach of privacy rights of the employees concerned. The employer may only process biometric data of its employees if such processing is justified by law or by an overriding public or private interest of the employer. With respect to the processing

[21] Some data protection considerations with regard to the use of biometric data in the private sector, *available in English at* http://www.edoeb.admin.ch/dokumentation/00153/00361/00366/index.html?lang=en.

[22] Sind Arbeitszeiterfassung und Zutrittskontrollen mit biometrischen Daten erlaubt?, *available in German at* http://www.edoeb.admin.ch/datenschutz/00763/00975/01213/index.html?lang=de.

[23] Leitfaden zu biometrischen Erkennungssystemen, *available in German at* http://www.edoeb.admin.ch/datenschutz/00628/00629/00637/index.html?lang=de.

[24] Datenspeicherung bei Verifizierungssystemen, *available in German at* http://www.edoeb.admin.ch/datenschutz/00628/00629/00637/index.html?lang=de.

of biometric data, the Commissioner explicitly mentions that consent is not a valid form of justification, as the employee is under a certain pressure and dependence due to the employment relationship. If the employer has a valid justification for using biometric data, the recognition system to be applied must be in line with the principles outlined in the guide on biometric recognition systems. Whenever possible, the employer shall make use only of biometric features that do not leave any traces and that cannot be collected without the knowledge of the person concerned (*e.g.* , contour of hand). Irrespective of the type of biometric feature used (fingerprint, contour of hand, face recognition, etc.), the employer shall not store such biometric data centrally, but rather locally on a security medium, *e.g.*, a chip, kept by each employee. The employer must take adequate security measures, such as encryption of biometric data, and must ensure that the error rate relating to recognition of individuals is negligible. The processing of biometric data must be made transparent. In particular, employees may request information on the processing of data relating to themselves and may request the destruction of such data.

900. Personnel Records

900.10. Personnel Records — In General

Data processing relating to personnel records must be conducted in accordance with the general data protection principles (see "*General data protection principles*" under Section 300.20.10, above). According to art.328*b* of the Swiss Federal Code of Obligations, "an employer may handle data concerning the employee only to the extent that such data concerns the employee's suitability for his or her job or is necessary for the performance of the employment contract."

900.20. Access to, and Correction of, Personnel Records

Any person may request information from the controller of a data file as to whether data concerning him is being processed (FADP art. 8, ¶ 1). Upon request, the controller of a data file must notify the data subject of: (a) all available data concerning the data subject in the data file, including the available information on the source of the personal data; and (b) the purpose of and, if applicable, the legal basis for the processing, as well as the categories of the personal data being processed, other parties involved with the data file, and the data recipient, if any (FADP art. 8, ¶ 2).

The private controller of a data file may refuse, restrict, or defer the provision of information where a formal legal provision so requires, or such refusal, restriction, or deferral is required due to overriding interests of third parties (FADP art. 9, ¶ 1). The private controller of a data file may also refuse, restrict, or defer the provision of information if his own overriding interests so require (*e.g.*, personal notes of the employer or personal data relating to pending procedures) on the condition that he does not disclose the personal data in question to third parties (FADP art. 9, ¶ 4; Guide on the Processing of Personal Data at the Workplace § 3.2.3). The controller of a data file must indicate the reason why he has refused, restricted, or deferred access to information (FADP art. 9, ¶ 5).

Private persons are, on complaint, liable to a fine of up to CHF 10,000 if they breach their obligations under FADP art. 8 - 10 by willfully providing false or incomplete information (FADP art. 34, ¶ 1, a).

Under the FADP, a data subject may also request that incorrect data be corrected (FADP art. 5, ¶ 2; Guide § 3.2.4).

900.30. Fees for Access to Personnel Records

Under the FADP, information sought from a data controller must "be provided in writing, in the form of a printout or a photocopy, and is free of charge" (FADP art. 8, ¶5). A payment may be required if the applicant has already been provided with the requested information in the 12 months prior to the application and no legitimate interest in the further provision of information can be proven. A legitimate interest is shown in particular if the personal data has been modified without notice being given to the data subject. A payment may also be required if the provision of information entails an exceptionally large amount of work. In any case, the costs may not exceed CHF 300. Applicants must be notified of the amount of the cost prior to receiving the information and may withdraw their request within 10 days (OFADP art. 2).

900.40. Retention of Personnel Records

Neither the FADP nor the OFADP contains any specific provisions or restrictions on the retention of personnel records. However, the Commissioner's Guide on the Processing of Personal Data at the Workplace provides generally that personnel records should be retained for a period of five years. Depending on the type of data, the retention period may be extended (see Guide § 3.3.1). In fact, according to prevailing legal doctrine, except for salary claims, which have a statutory limitation period of five years,

other claims relating to the employment contract have a statutory limitation of 10 years, justifying a longer retention period on a case-by-case basis. As a rule, personal data should be destroyed as soon as it is no longer needed (Guide § 3.3.1). In particular, after termination of an employment relationship, the employer may only retain data that is still required (*e.g.*, as evidence in connection with potential claims which are not yet time-barred, for social security or tax purposes, or due to general bookkeeping requirements).

The data handler must ensure that the personal data is being stored in a secure manner and that access is granted only to those persons within the company who need to have access (*e.g.*, HR personnel).

900.50. Disclosure of Personnel Data to Third Parties

The Commissioner's Guide on the Processing of Personal Data at the Workplace notes that disclosure of personal data to a third party can quickly lead to a violation of privacy and should be handled with caution (Guide § 3.2.5). Sensitive personal data and personality profiles may not be disclosed to third parties for such third parties' own purposes (including group companies or potential new employers after notice of termination) without justification (Guide § 3.2.5). Possible forms of justification are consent (*n.b.*, employees may consent only within the limits set forth by CO art.328*b*), an overriding private or public interest, or other provisions of law (*e.g.*, relating to social security; FADP art. 12, ¶ 2, c and art. 13, ¶ 1). According to the Guide (§ 3.2.5), these strict rules apply not only to sensitive personal data and personality profiles, but also to all other employee-related personal data.

The disclosure of employee data to third parties who process such data on behalf and for the purposes of the employer (*e.g.*, a company providing payroll services to the employer) generally does not require the prior consent of the employees concerned. Such assignment is permitted if the assignee processes the personal data exclusively in the manner permitted for the assignor and if the assignment is not prohibited by a statutory or contractual duty of confidentiality (FADP art. 10*a*, ¶ 1, a and b). Furthermore, the assignee must in particular guarantee the security of the personal data (FADP art. 10*a*, ¶ 2). Also, the general data protection principles, in particular the principle of transparency, must be observed (see "*General data protection principles*" under Section 300.20.10, above). An assignment must be made based on an agreement (*cf.* FADP art. 10*a*, ¶ 1). Although the FADP does not require an agreement to be made in writing, doing so is strongly recommended and is regularly seen in practice. A processing agreement need not be a separate document, as it can be integrated into an underlying business agreement.

Particular requirements apply to disclosures abroad. In fact, personal data may not be disclosed abroad if the privacy of the data subject would be seriously endangered thereby (FADP art. 6, ¶ 1). Such a danger may in particular occur if personal data is disclosed to a country whose legislation does not guarantee an adequate level of protection for personal data. The Commissioner has published a non-binding list of countries that provide an adequate level of data protection with respect to individuals, but the list does not generally indicate whether the respective country provides an adequate level of data protection with respect to legal entities. As a rule, most countries have not implemented protection for legal entities in their national data protection laws and therefore cannot *per se* be considered as providing an adequate level of protection for personal data pertaining to legal entities.

If personal data is disclosed to a country that does not provide an adequate level of data protection for the type of personal data being transferred, such disclosure may only occur if:

(a) sufficient safeguards, in particular contractual clauses (typically the EU Model Contract Clauses adapted to Swiss law requirements), ensure an adequate level of protection abroad (FADP art. 6, ¶ 2(a));
(b) the data subject has consented in the individual specific case (FADP art. 6, ¶ 2(b));
(c) the processing is directly connected with the conclusion or performance of a contract, and the personal data relates to that of a contractual party (FADP art. 6, ¶ 2(c));
(d) disclosure is essential in the specific case at hand in order to either safeguard an overriding public interest or for the establishment, exercise, or enforcement of legal claims before the courts (FADP art. 6, ¶ 2(d);
(e) disclosure is required in the specific case to protect the life or physical integrity of the data subject (FADP art. 6, ¶ 2(e));
(f) the data subject has made the data generally accessible and has not expressly prohibited its processing (FADP art. 6, ¶ 2(f); or
(g) disclosure is made within the same group of companies, provided those involved are subject to data protection rules that ensure an adequate level of protection, (*e.g.*, through the adoption of binding corporate rules [BCR]) (FADP art. 6, ¶ 2(g)).

If the disclosure is based on the measures mentioned in items (a) and (g) above, the Commissioner must be informed about the contractual safeguards or the BCR that have been adopted before such transfer

abroad takes place for the first time (FADP art. 6, ¶ 3). Private persons are liable to a fine of up to CHF 10,000 if they willfully fail to provide the Commissioner with the information required by FADP art. 6, ¶ 3 or who in doing so willfully provide false information (FADP art. 34, ¶ 2(a).

In general, consent does not justify disclosure of employee data to a country without adequate data protection legislation, for it is unclear to what extent such consent would be valid in the context of disclosure of employee data (see fifth bullet point under Section 300.20.10, above). Furthermore, consent could be withdrawn at any time by the employee concerned, and, in any event, it proves to be difficult in practice to ensure that all employees have in fact given their consent to disclosure abroad.