Data protection and protection of personality rights

This fact sheet is intended to provide you, as a vocational trainer, with an insight into the complex subject of data protection and protection of personality rights. The topics that are most likely to raise questions during vocational education and training are briefly summarised and explained. To help you find out more, important addresses and further links are listed at the end of this fact sheet.



Data protection in the workplace

In the employment relationship, large volumes of employees' personal data are collected, evaluated and shared both within the company and with external parties. Employees therefore have a significant interest in ensuring that their personal data is processed in accordance with the law and that their personality rights are not unlawfully infringed.

Data processing in the workplace is also of great importance from a company perspective: in addition to managing the employment relationship, it also serves other important purposes of the company, such as personnel development and management, the efficient use of the company's resources and compliance with applicable laws.

It is therefore important for everyone involved in vocational education and training – vocational trainers and learners – to be aware of the legal regulations that are relevant to them and to implement them in their day-to-day professional and private lives.

Legal basis Data protection

The purpose of data protection is to protect the personality rights and fundamental rights of natural persons whose personal data is processed. In Switzerland, the Data Protection Act (FADP), the Data Protection Ordinance (DPO) and, where applicable, the EU General Data Protection Regulation (GDPR) apply in particular. If specific laws contain data protection provisions, they take precedence as more specific regulations and supplement the FADP (for example Art. 328b CO governing the processing of employees' personal data. The FADP remains applicable in all other respects).

Application documents

Submitted application documents may only be viewed by those responsible for recruitment (vocational trainers, direct supervisors, HR department). Only information required to assess a candidate's suitability for the position may be requested. Applicants' application documents must be returned or deleted in full, unless the data subject gives their consent to keep the documents for a specified, proportionate period of time. The documents must be destroyed as soon as they are no longer required for the agreed purpose. It is advisable to obtain consent in writing for evidentiary purposes.

Legal basis: FADP Art. 6, CO Art. 328b

© 2026 SDBB, Bern

Personnel files

Host companies can create personnel files for their learners and employees, provided they comply with the obligation to inform those concerned. When collecting personal data, the controller, i.e. in this case the host company, must inform the data subject appropriately about the collection of their personal data.

Only data relating to the suitability of the employee for the employment relationship or which is necessary for the execution of the employment contract may be processed. Information about an employee's private life, membership in a trade union or derogatory comments about them may not be included. With regard to health, only data that is directly related to the employment relationship may be included in the personnel file (e.g. medical certificates with details of the duration and degree of incapacity for work, but without the diagnosis)

Legal basis: FADP Art. 19, CO Art. 328b

Technical and organisational measures

Every data processor is obliged to take appropriate technical and organisational measures (TOMs) to protect personal data against unauthorised processing and data loss. Which specific TOMs are taken must be determined on a case-by-case basis; however, the measures must be suitable for preventing data security breaches.

TOMs can be, for example: access controls, keys, ID cards or password authentication. In particular, vocational trainers should make students aware that they use a strong password that they do not pass on or write down.

Legal basis: FADP Art. 8, DPO Art. 1–6

Third-party processing (processing)

If the host company outsources the processing of personal data to third parties (e.g. to a cloud provider, payroll or HR software or an external IT service provider), it remains responsible for this. Processing by a processor is only permitted if the processor only processes the data in the same way that the host company itself would be permitted to do. The host company must also ensure that the processor guarantees data security. However, if data is disclosed abroad, the following rules apply.

Legal basis: FADP Art. 9

Disclosure of personal data abroad

If personal data is disclosed abroad (e.g. when using foreign cloud or software services), this is only permissible if appropriate data protection is provided in the target country. The countries to which this applies are listed in the annex to the DPO. In the absence of adequate protection, appropriate safeguards are required.

Legal basis: FADP Art. 16 and Art. 17

Provision of information

Whether the company may disclose employees' personal data to third parties must be examined on a case-by-case basis.

The host company must obtain the consent of the learner for any information it discloses about a learner or employees, unless there is an overriding private or public interest or the law justifies such information.

Legal basis: Art. 31 FADP

The collaboration between the host company and the VET school is governed by Art. 16 para. 5 VPETA. Art. 17 para. 3 VPETO must be observed with regard to contact between the VET school and the host company in the event of unsatisfactory academic performance or unsatisfactory conduct.

There are statutory reporting and disclosure obligations vis-à-vis the cantonal VET office: The host company must submit the apprenticeship contract for approval and immediately report the termination of the apprenticeship contract. The VET office also oversees vocational education and training; this also includes advising and supporting the contracting parties (depending on the canton, for example, by vocational training inspectors or training advisors). As part of this supervision, the host company may provide the VET office with the necessary information about the learner (VPETA Art. 14 para. 3 and 4 VPETA, Art. 24).

Rights of data subjects

Data subjects – external or internal persons, e.g. employees – may assert certain rights vis-à-vis the company, which the company must uphold.

The rights of the data subject are in particular: the right of access, the right to rectification of incorrect data, the right to erasure or destruction and (in the event of disputes) the right to have a note of dispute added and the right to receive and transfer the data.

Particularly important is the right of access, according to which every person can request information from the controller as to whether personal data concerning them is being processed.

Legal basis: FADP Art. 25, Art. 28 and Art. 32

Dealing with data security breaches

If data security is breached (“data breach”) and an individual suffers loss or damage as a result, the controllers may be held liable. A data security breach must be reported to the Federal Data Protection and Information Commissioner (FDPIC) as quickly as possible if the breach results in a high risk to the personality rights or fundamental rights of the employees concerned. If requested by the FDPIC or if it is necessary to protect the data subject(s), they must be informed.

Legal basis: FADP Art. 24

Protection of personality rights and conduct in the company

All companies are obliged by law to protect the personality rights of their employees and to ensure that their conduct within the company reflects this obligation. The protection of personality rights concerns the individual person (learner, vocational trainer, employee) and grants them rights to which they are entitled by virtue of being an individual and are inextricably linked to them. It goes without saying that all vocational trainers and learners must also comply with this obligation. If personality rights are violated – for example, if a learner uses violence, makes threats or harasses others – the host company or vocational trainer must intervene.

The same applies if the injury is caused by a vocational trainer or other employees, e.g. by verbal abuse, bullying or sexual harassment. In this case, the host company must take the necessary measures to protect the learner. Learners affected can contact a person of trust in the company (e.g. the vocational trainer’s line manager, the management or the HR department). Outside the company, the VET office in particular is the point of contact. It advises and supports the contracting parties and mediates in the event of conflicts.

General duty of care

All companies must respect and protect their employees' personality rights, take due account of their health and ensure that appropriate standards of decency are maintained. This general duty of care specifies the general protection of employees' personality rights with regard to the employment relationship.

Legal basis: CO Art. 328

Monitoring in the workplace

General:

Monitoring is generally inadmissible if it is intended to monitor employees' conduct at the workplace, if it impairs employees' health and freedom of movement, or if the general requirements of Art. 328b CO and data protection are not complied with.

However, monitoring may be permissible if it is proportionate. This means that the interests of the employee and those of the company must always be weighed up. The employee's interests primarily concern the protection of their personality rights, which are balanced against the company's interests, such as the safety of employees and third parties or compliance with legal regulations.

It is important to have clear usage regulations that are communicated to learners and employees.

Technical monitoring:

Technical monitoring (e.g. by video or software) is only permitted for security purposes. Employees must be informed of this in advance and give their consent, or there must be a public interest or a corresponding legal basis.

Employees must not be monitored around the clock.

In order for vocational trainers to be able to monitor internet use, they need specific indications that, for example, illegal websites containing pornographic or racist material or incitements to violence have been accessed or that there has been serious misuse for private purposes.

The company may not systematically monitor employees' work-related e-mail correspondence. Monitoring of work-related e-mail correspondence must be proportionate and serve a specific purpose. Personal e-mails may not be read.

Legal basis: CO Art. 328b, EmpO 3 Art. 26 para. 1, FADP

Mobile phones

Vocational trainers and teachers at VET schools can prohibit learners from using mobile phones at the workplace during working hours or in the classroom. The devices may be temporarily confiscated, but must not be checked for content. This applies to the workplace (e.g. construction site) as well as to the classroom.

Monitoring of telephone conversations

Monitoring and recording telephone conversations is only permitted in exceptional cases, e.g. for assessing performance or for training purposes (e.g. in a call centre) or for security reasons, and must be proportionate. Learners and employees must be informed of this in advice and give their consent. In principle, the other parties to the call must also be informed in advance (e.g. by means of an announcement at the beginning of the call). Private conversations may not be monitored or recorded. Anyone who monitors or records conversations without the required consent may be liable to prosecution. Call meta data (e.g. time and duration of calls) may be recorded and analysed by the company insofar as this is proportionate.

Clothing and appearance

Vocational trainers and host companies can only issue instructions to learners if there is a direct impact on their work (e.g. safety, hygiene, customer contact). However, such measures must always be proportionate.

Notification of persons with parental responsibility (legal representative, usually parents)

In the case of learners under the age of 18, vocational trainers are entitled to consult persons with parental responsibility (legal representative, usually parents) for a discussion or to clarify a situation, even against the learner's will. If the learner is of legal age, consent must be obtained. The rights of the non-custodial parent may be restricted, in particular with regard to their involvement. It is therefore advisable to clarify communication with parents living separately as early as possible.

Legal basis: CO Art. 345 para. 2, CC Art. 275a para. 2, CC Art. 296 et seq.

Skills testing

Selection procedures must enable objective, reliable and meaningful results. Tests (personality tests, psychological skills tests, graphological reports) may only be conducted if they are used to determine suitability for the occupation. Psychological skills tests may also only be carried out during the application procedure with the consent of the applicant and only to the extent necessary to assess their suitability for the planned work assignments.

Skills testing may only be carried out and evaluated by qualified external specialist authorities or by in-house specialists.

Tests used to check occupation-related content can be conducted by the vocational trainer.

Alcohol and drug testing

Alcohol and drug tests may be ordered by the employer as a preventive measure in certain cases. However, this is only possible under certain conditions, in particular where safety considerations outweigh the employee's personality rights and the employee has given their consent.

Alcohol and drug tests may only be carried out on a random basis and only as part of a set of safety measures described in the employment contract or in a regulation that forms an integral part of that contract.

Alcohol and drug tests may only be carried out with the explicit consent of the learner or the applicant, as there is no legal basis. If consent is not given, the individual cannot be forced to undergo testing, but may face consequences under employment law in certain circumstances where safety considerations outweigh the individual's interests or rights.

Invasive alcohol and drug testing must be carried out by healthcare professionals. They may only inform the employer whether the employee is fit to perform their duties.

Breathalyser tests may also be performed by other persons.

The costs of tests ordered by the host company are generally borne by the host company.

Legal basis: CO Art. 328 and Art. 328b, EmpA Art. 6, AIA Art. 82, APO Art. 11 para. 3, FADP Art. 6

Health checks

Health checks may only be carried out with the explicit consent of the learner or the applicant.

In some occupations, a professional medical examination is required. It is carried out before the start of the apprenticeship and is required to confirm that the individual meets the health

requirements for vocational education and training. The company must not have access to such documents. Doctors may only provide information about the suitability of the applicant for the position to be filled.

Legal basis: EmpO 5 Art. 9, EmpO 5 Art. 18

As a vocational trainer, raise important issues

The way in which we communicate has changed rapidly in recent years. Digital media have become an integral part of our everyday lives. They offer a wide range of learning and development opportunities, but they also pose risks. Many people – especially young people – use social media to connect with their friends. Although they are aware that these platforms are also publicly accessible to people other than their friends, they are often unclear about the possible consequences. Without giving it much thought – and generally without malicious intent – they also upload sensitive data, such as photos or videos with questionable content (revealing images, drinking binges, damage to property, etc.) that they often take without the consent of the person concerned, thereby infringing their personality rights.

Sometimes young people post accusations, insults or derogatory comments about colleagues but also against teachers or employers online. These may include comments made in frustration that they themselves regret shortly afterwards. They discriminate against others, make ill-considered (sometimes also deliberate) racist and/or sexist remarks.

Young people send sensitive comments in messages or e-mails – without giving it much thought and not intentionally – which can be forwarded at any time by others to unauthorised persons or the parties concerned or can be simply uploaded to the internet.

Completely removing this data with problematic content is not as easy as publishing it. It can remain accessible for years or be shared further by others. Since texts, pictures or videos can be viewed in a completely different light after a long time and can be difficult to deny, they may unexpectedly cause problems in a person's professional career or private life.

Learners should therefore be made aware:

- that they are obliged to protect the personality rights of their supervisors and employees of the host company (photos, videos and statements about others or by others may not be taken or published without the consent of the persons concerned).
- that they must comply with the host company's data protection regulations (e.g. not passing on sensitive data).
- how critical it can be to publish personal data – their own or that of others – on the internet (photos, statements, opinions, etc.).
- that they should not publish compromising data about others.
- that data published online can only be deleted from specific locations.

On the other hand, vocational trainers can also tell learners to speak up if others use sensitive data (whether genuine or fake) to put pressure on them or bully them. For example, sexting. This refers to the sending of erotic or pornographic messages or sexually explicit images of oneself using a mobile phone or computer, which in itself is not yet a criminal offence. However, if the recipient uses the images as a means of extortion and blackmails the sender into sending further images or even engaging in sexual acts, they are committing a criminal offence.

Legal basis

FADP, Data Protection Act (Federal Act of 25 September 2020 on Data Protection, SR 235.1)

DPO, Data Protection Ordinance (Ordinance of 31 August 2022 on Data Protection, SR 235.11)

CO, Swiss Code of Obligations (Federal Act of 30 March 1911 on the Amendment of the Swiss Civil Code – Part Five: Code of Obligations, SR 220)

CC, Civil Code (Swiss Civil Code of 10 December 1907, SR 210)

SCC, Criminal Code (Swiss Criminal Code of 21 December 1937, SR 311.0)

EmpA, Employment Act (Federal Act of 13 March 1964 on Employment in Business, Trade and Industry, SR 822.11)

EmpO 3, Ordinance 3 of 18 August 1993 to the Employment Act (Healthcare, SR 822.113)

EmpO 5, Ordinance 5 of 28 September 2007 to the Employment Act (Youth Protection Ordinance, SR 822.15)

VPETA, Vocational and Professional Education and Training Act (Federal Act of 13 December 2002 on Vocational and Professional Education and Training, SR 412.10)

VPETO, Vocational and Professional Education and Training Ordinance (Ordinance of 19 November 2003 on Vocational and Professional Education and Training, SR 412.101)

(Laws can be accessed with SR numbers at: → *fedlex.admin.ch*)

Important links

→ *vocationaleducation.ch/addresses*
List of cantonal VET offices. Point of contact for initial information and referral to specialist units.

→ *vocationaleducation.ch/glossary*
All important VET terms are described in short and informative texts.

→ *centrepatronal.ch*
Centre Patronal represents the concerns of employer organisations, trade associations and other institutions and publishes “The Employer’s Handbook”, a reference guide for anyone who deals with employment law issues in their professional work.

→ *datenschutz.ch*
Website of the Canton of Zurich's Data Protection Officer. The data protection app can be downloaded from the website.

→ *edoeb.admin.ch*
Informative website of the Federal Data Protection and Information Commissioner (FDPIC), which contains helpful guides, leaflets, recommendations and teaching materials for use with young people.

→ *jugendundmedien.ch*
Informative website for young people and vocational trainers. Here you will find answers to questions such as: What opportunities and risks are associated with the use of digital media? How can media literacy be promoted? How do you protect yourself from potential risks?

→ *privatim.ch*
Website of the "Association of Swiss Data Protection Officers" with addresses and links to all cantonal data protection officers

→ *suva.ch*
"Suchtmittel am Arbeitsplatz aus rechtlicher Sicht" (Addictive substances in the workplace: legal aspects, not available in English). Informative brochure available for download.

October 2026 Edition
This and other fact sheets can be found at:

→ *vocationaleducation.ch/factsheets*

© SDBB Bern
Reproduction in whole or in part, including use in digital media, is permitted for non-commercial purposes provided the source is acknowledged.