Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Hinweis

Die englische Version der von der Datenschutzkonferenz beschlossenen "Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattform im Schulunterricht" wurde auf Veranlassung des Thüringer Landesbeauftragten für den Datenschutz und die Informationsfreiheit übersetzt.

A Guidebook[1] From the Data Protection Supervisory Authority for Online Learning Platforms in School Classrooms

Last revised: May 25 2018

[1] Decided on the 95th Conference on Data Protection April 24-26, 2018 with opposing vote from the Bavarian state representative for data protection

1. Objective

Educational institutions increasingly rely on web-based transfer of knowledge as well as electronic possibilities of communication between teachers and learners. Correspondingly, schools progressively utilize online learning platforms in classes. These online learning platforms are made available by school supervising authorities, publishers of school books, computer and software producers, and other providers. The advantages of those practices are justified by their time and location-independent usage. However, at the same time large amounts of data from teachers and learners are being processed. The guidebook at hand is specifically directed at schools which aim to deploy online learning platforms as educational tools. These guidelines should serve as an outline for (minimum) requirements with regard to the necessary data protection regulations in handling online learning platforms. Such guidelines also allow online learning platforms providers to design and adapt their respective product accordingly so that its usage is admissible for schools.

Online learning platforms should serve to support the educational task of schools e.g.

Competence orientation
Integration of technical, methodical and social educational objectives
Processuality of the learning method
Support for learners in small groups
Promoting abilities according to individual aptitude
Recognition of individual learning progress and learning difficulties
Consultation and learning promotion of single learners

In addition, it should also be noted that the work groups Technik und Medien (Technology and Media) from the German federal and state representatives for data protection and Internationaler Datenverkehr des Düsseldorfer Kreises (International Data Traffic of the Düsseldorf

Group) compiled a guidebook called *Cloud Computing* that illustrates the special requirements for web-based applications i.e. data processing in the cloud. Online learning platforms used for other than educational purposes are not subject of the guidebook at hand.

2. Definition

Online learning platforms according to the guidebook at hand are software systems that supplement or even substitute teaching in that they offer and organize learning contents. However, software systems that are used for school management tasks are not system related to the online learning platforms according to the guidebook at hand and must be regarded separately.

Schools might organize the virtual learning environment of online learning platforms to set up communication, group work, assignments and grading reports. Accessing the software functions location independent via an internet browser on an online terminal (e.g. PC, Tablet etc.). First, a user profile must be created for every participating learner. According to the user profile the online learning platform system then creates an individual user account. Furthermore, the school i.e. the responsible teacher must set the individual access permissions for the respective user account and configure the features of the online learning platform (provision of learning content, discussion forums, assignments etc.). Before any use and in order to be able to take a specific course, learners from a particular grade or year need to, according to their specific subject, register online on the learning platform.

3. Data-Protection Law Issues

In general, users individually log in on online learning platforms, and their online behavior is being logged repeatedly. Among other things, the compiled data documents when and which user, accessed what websites, if and what course had been chosen and how it was graded. Thus, individual learner profiles are being created.

Legal school regulations for data handling and usage of individual-related data require that the compiled data must be relevant for a School in adequately performing their guided tasks. Many online learning platforms offer more possibilities for evaluating data than necessary for a school to perform their guided tasks and thus need to be adjusted accordingly.

In using online learning platforms, teachers also need the possibility to monitor the individual learning progress of learners to specifically assist learners in individual consultations or in planning and realizing interventions conductive to their learning situation. Advanced details about learners of an online learning platform e.g. how often and at what times they participated in assignments must not be made accessible in this regard. Before using online learning platforms, learners, and if necessary their parents or legal guardians, must be informed about existing data evaluation possibilities of the respective application and which consequences this may bear with regard to user behavior.

Conclusion:

- Online learning platforms must be configured to only collect and process data that is necessary for the school to fulfill its pedagogical tasks
- It is therefore recommended to use online learning platforms that can be modularly adjusted to the intended application scenario
- Before using online learning platforms, data subjects must be informed comprehensively about possible data evaluations

4. Legal Bases

The legal basis for the processing of personal data of learners also in online learning platforms is primarily Regulation (EU) 2016/679 of April 27 2016 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data, on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation - GDPR). Via the opening clause in Art. 6(1)(b) GDPR, the respective school laws, school data protection laws, and related ordinances are to be applied, provided that they are to be brought in line with the GDPR, which has been directly applicable since May 25 2018.[2] The obligatory use of an online learning platform can only be prescribed by or on the basis of a law. It is conceivable, for example, that it could be designated as a teaching aid by means of a corresponding ordinance on the basis of statutory authorization. Otherwise, such a platform may only be used on the basis of voluntary consent.[3] The requirements for legal consent in accordance with Art. 7 GDPR must be respected.[4]

[2] This is to be assumed in principle. In case of doubt, it is recommended to contact the responsible data protection supervisory authority.

[3] According to Article 8(1), information society services offered directly to the child require the consent of the child at the age of 16. Moreover, consent is not unproblematic with regard to recitals number 32 and 43. According to this, consent solutions are possible to a limited extent in a subordination relationship, since the mandatory prerequisite of voluntariness is not unequivocally guaranteed. In each individual case it must be reliably checked and it must be ensured that the data subjects have actually made their decision free of pressure or coercion. When personal data are processed for teaching purposes or in connection with the performance and evaluation of pedagogical tasks in classrooms, it is extremely difficult to assess voluntariness.

[4] In this regard, see Guidelines on Consent under regulation 2016/679, WP 259, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48849

Conclusion:

Before employing an online learning platform, it must be ascertained whether its use is legally permissible and whether the students and, if necessary, their parents or legal guardians must give their consent to the use of the platform.

5. Responsibility

According to Art. 4(7) GDPR, the responsibility lies with the body that alone or together with others decides on the means and purposes of processing personal data. The decisive factor is which body decides on the basic use of the online learning platform and the detailed circumstances of its implementation. In this respect, it is irrelevant where the data are being processed. The person responsible must be able to determine the way in which the data is processed, i.e. remain "master of the data". Teachers may only employ online learning platforms in the context of leisure time and the organization of lessons to the extent that the school or the school supervisory authority has decided on with regard to the use of the respective online learning platform.

6. Extent of Data Processing

6.1 Mandatory Data

The school or the school supervisory authority must determine which data is absolutely mandatory for the use of the online learning platform.

6.1.1 Mandatory Master Data

- Name and address of the respective school and the persons in charge, who may vary when the school supervisory authority performs this task.
- Master data for creating user accounts that serve both to identify the user in the system and to assign functions and authorizations. It is possible that the user enters and sets up the data or that the data is recorded or changed by the school. It is important that only

data which are necessary for the meaningful use of the educational task fulfilment of the school can be entered.

- The user administration by the administrator has to distinguish between the user name and the logon name. The user name must contain the real name (genuine name) of the user. The genuine name is required for the identification of a learner by supervising teachers and does not have to exactly correspond to the logon name. The logon name is used when logging on to the system and should not correspond to the user name. On the contrary: according to Art. 25(1) of the General Data Protection Regulation, suitable technical and organizational measures such as pseudonymization should be taken, which, in turn, effectively implement the data protection principles such as data minimization. The logon name can be chosen freely. The registration with pseudonyms is an advisable precaution to make the misuse of the account by third parties more difficult.
- The specification of an email address is optional or mandatory, depending on the system. An email address is used in particular to send notifications from the courses taken and to request a new password if it is lost. For security reasons, a password reset may not be based solely on email notifications. The assignment of an internal email address is generally recommended because otherwise personal data from the controlled area of the online learning platform can reach unauthorized persons via notifications.

A user account can contain additional information that facilitates communication within the system, such as grade level, learning group name, learning course (e.g. at vocational schools).

Conclusion:

- When selecting online learning platforms, it is important to ensure that the principles of data economy and data avoidance (e.g. not too many master data, free text fields, comment functions) are ensured.
- A pseudonymized user administration is recommended.

6.1.2 Optional Data

Further optional data can be entered in the user profile on a voluntary basis by the user. In this respect, fields such as "description", "profile picture" and "fields of interest" deserve attention in particular.

Optional data fields for common online learning platforms can be:

- Time Zone: This field is usually deactivated or assigned a default value, since all users usually live in the same time zone.
- Description: Users can enter their personal details into this field. This information is visible within the online learning platform, but not publicly. This field is not required and should be deactivated.
- Profile picture: The user can upload an image file (e.g. a portrait photo) for which he owns the copyrights. This field is not required, it bears the risk of possible infringements and should therefore be deactivated.
- Website: Course participants can enter an URL to their own homepage here. This field should be deactivated.
- Preferred language: This setting allows to display user interfaces in languages other than German. Usually, this field is not required and should be deactivated.
- Institution, Department: This information is not usually used at school.

For organizational purposes, additional optional data fields can be created and maintained. This is only permissible insofar as it is necessary for the fulfilment of educational tasks. For example, it would be possible to specify which courses a learner attends in order to gain access to the relevant documents. This does not include personal information such as hobbies or private telephone numbers.

6.1.3 Usage Data

When using an online learning platform, data about the user and his activities are automatically logged and stored. This log data is stored on the server and must only be used for monitoring the functionality and security of these systems, and in cases of illegal misuse by third parties. In addition, reference is made to the latest version of the orientation guide *Protokollierung* (Logging) from the Arbeitskreis Technik (Working Group on Technology) of the federal and state representatives for data protection. Further details should be specified in the usage regulations. Usage data are generally not required for the performance of school tasks and should therefore only be accessible under strictly determined conditions and for clearly defined groups of persons and purposes. Usage data are for example:

- Registration status: first login in the system, last login, time of log out
- Logging of entries and changes
- IP-Addresses, services used (e.g. file downloads, chat)

6.1.4 Pedagogical Process Data

Pedagogical process data is information that enables the teacher to understand the individual and group learning process. Pedagogical process data are used for planning didactic interventions, for reflection, evaluation and further development of the classroom and for planning individual learning consultation for individual learners or small groups. In different modules of an online learning platform process data are generated, which are visible for different groups of people. Such modules are:

- *Forum discussion:* Forum posts can be associated with the authors and arranged in chronological structure. In addition, the depicted structure displays to which post an answer was given. This information is visible to all users. However, a display of posts that have not yet been read is only visible for the respective individual user.

- *Wiki Entries:* A wiki is a multi-page document written by different authors of a course. By logging the history, it is possible to determine who edited which parts of a document. This allows the teacher to track the participation and contributions of individual learners. This is important for feedback, grades and to promote social and communicative aspects of learning.
- *Glossary (Database):* The glossary is a structured collection of information. It contains individual text entries with information about the author and the time of creation. These details are visible to everyone.
- *Training objects (Assignments, Exams):* Depending on the type of object, different data are only visible to teachers or also to individual learners. In this regard, the visibility of the data for teachers must be pedagogically justified and determined by the school management or the school conference. Monitoring of extracurricular activities of learners by teachers is not allowed.
- *SCORM-Modules, LTI-Modules, Live Classroom, Plagiarism Check etc.:* When using such modules, personal data may be transferred to external service providers. This is only permissible within the framework of existing order processing contracts between schools and/or school authorities and providers and must be reviewed separately under data protection law. Process data of learners may only be visible to other participants if this is methodically or didactically necessary. An example of this is the rating function in a discussion forum. Depending on the implementation, it allows fast, possibly non-verbal feedback on contributions. Since verbal evaluation functions can also be used for inappropriate and offensive criticism of fellow learners without the teachers being able to intervene in time, such a function should only be activated with caution.

6.1.5 Statistical Data

Online learning platforms allow the evaluation of statistical data, for example on the type and scope of use. However, genuine statistical data have no personal reference and are therefore unproblematic in terms of the protection of data privacy. If it is not genuine statistical data in this meaning, the respective school laws, school data protection laws and the relevant statutory regulations of the respective states apply to them.

6.2 Written Specifications

Before using the online learning platform, the school or the school supervisory authority must make written specifications on permissible data use including a profile and authorization concept. The information necessary for the procedure must be provided in accordance with Art. 30 GDPR in the list of processing activities.[5]

The requirements for the configuration and application of online learning platforms by administrators and teachers can, for example, take the form of a user regulation which clearly regulates how confidentiality, integrity, authenticity, the non-linkability of data and the intervention capability of the user are to be implemented locally in accordance with the respective applicable federal state law. This includes the deletion concept (see section 9.9) and the question which email address are used (see section 9.2).

Conclusion:

The general principles of the data processing procedures must be defined in a user regulation agreement before deploying the online learning platform.

[5] For more information, please refer to Brief Paper No. 1 of the Data Protection Conference https://www.tlfdi.de/mam/tlfdi/themen/dsk_kpnr_1_verzeichnis_verarbeitungstatigkeiten.pdf

7. Necessary Checks

7.1 General Evaluation of the Protection Needs of the Processed Data

If data are processed by a responsible data supervisor (see section 6), it is necessary to define the need for data protection. From this specification it is then possible to take the necessary protective measures (see section 9 [not conclusively]) to protect the rights of data subjects concerned. In order to define the need for protection and the measures to protect the rights of the data subjects, the data protection supervisory authorities have developed the Standard-Datenschutzmodell (SDM) (Standard Data Protection Model [SDPM]) as a practical aid. This model is available for download on the websites of the data protection supervisory authorities. The SDPM methodology can also be used as a tool for the data protection impact assessment in subsection 7.2.

7.2 Data Protection Impact Assessment

Before using online learning platforms, the data controller (school or school supervisory authority) and his data protection representative must check whether the data processing is likely to bear a high risk with regard to the rights and liberties of concerned natural persons (learners, teachers, parents). Due to the nature of the circumstances and the purposes of the data processing in an online learning platform, this is generally to be assumed.[6] The person responsible must then, in advance, carry out a data protection impact assessment in accordance with Art. 35 GDPR. The person responsible must obtain the advice of his data protection representative but remains solely responsible for the implementation. The following aspects in particular must be taken into account with respect to the data protection impact assessment:

- Compliance with existing state regulations on the use of online learning platforms

[6] see the Standard Data Protection Model in version 1.0 — test version

- When purchasing an online learning platform from an external service provider, it must be examined whether the provider can meet the data protection and school requirements.
- Configuration and selection of data processing systems according to the principles of data avoidance and data economy

7.3 Contract Processing

When using external service providers, the legal requirements for contract processing in accordance with Art. 28 GDPR must be observed. The following general requirements apply:

- The school or school supervisory authority must remain the "master of the data". The School or school supervisory authorities determine who processes and uses the data and in what way this will occur. The school or school supervisory authority must have the right to direct the contractor with regard to data processing and data use and must be granted control rights by contract.
- The general terms and conditions of external service providers must be reviewed in accordance with the principles outlined in the guidebook at hand and, if necessary, modified by contract.
- A contract must be negotiated with the order processor which meets the data protection requirements for order processing in accordance with Art. 28 GDPR.[7]

7.4 Other Requirements

- The principle of earmarking applies. In particular, it must be ensured that the data of learners, teachers and parents are not used for advertising purposes.

[7] For more information, please refer to Brief Paper No. 13 of the Data Protection Conference https://www.tlfdi.de/mam/tlfdi/themen/kurzpapier_nr.13_auftragsverarbeitung.pdf

- The conditions of use to be drawn up by the school or school supervisory authority and the list of processing activities (Art. 30 GDPR) as well as other technical and organizational measures taken must be reviewed in terms of data protection laws.

8. Information, Notification, Training and Instruction Obligations

Learners, parents[8] and teachers must be informed in detail about the type, scope and purpose of the data collected, processed and used before the usage of online learning platforms. In this respect, the requirements for the information of the data subjects according to Art. 13 and 14 GDPR must be observed.

If consent is required for the use of certain modules then learners, parents and teachers must be expressly informed of the voluntary nature and the existing right of withdrawal and its legal consequences (see section 4). The consent must be obtained in such a way that the person responsible for data management can verify compliance with the respective legal requirements (e.g. in writing). The consent must indicate which data are to be processed, in what form and for what purpose. In addition, users must be informed as to whether and to whom data is transmitted. The declaration of consent must be made available by the person responsible in intelligible, concise and simple language (see recital 42 GDPR). In addition, teachers and administrators must be trained accordingly and learners must be appropriately instructed.

[8] Depending on the applicable state law, it may be possible that parents of adult learners are not always granted access rights.

9. Notes on Technical and Organizational Implementation

9.1 Passwords

The use of an online learning platform requires password-protected access. Passwords must be securely stored cryptographically, e.g. by employing a password-based key derivation function. Areas with special categories of personal data according to Art. 9(1) GDPR should be secured with a two-factor authentication (2FA). It must be guaranteed that nobody within the online learning platform is able to read passwords in plain text. This also applies to administrators.

If the school assigns passwords, it must be ensured that the user is obliged to change the previously assigned password when logging in for the first time. Deviations from this rule may be made in justified individual cases, for example in the case of primary school children or learners with needs for a special support. Users with administrative rights to edit user accounts in the system can reset passwords for other users. It is not recommended to assign new passwords, as the administrator will then become aware of the new password. When generating passwords, using passwords and managing passwords, it is recommended to refer to the M 2.11-Regelung des Passwortgebrauchs (M 2.11 regulation for password usage) published in the IT-Grundschutz-Kataloge (basic IT protection catalogues) by the Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security). This concerns in particular the complexity of the password and the duty of confidentiality. A given regular password change can be useful in this context. However, this depends on the individual framework conditions. The minimum number of characters and their composition (number of uppercase letters, number of lowercase letters, number of digits and number of special characters) must be specified for the use of passwords. When defining these requirements, the age of the learners must be taken into account in order not to create access problems. However, a password should never be shorter than eight characters.

9.2 Email Address

The email address is a distinct parameter. If an email address is to be made available within the online learning platform, it must be ensured that it cannot be used for several user accounts. The use of email addresses must be specified in writing.

9.3 Entry of User Account Data and Modifiability

User accounts can be created by importing, manually entering or connecting to an existing database according to the systems used in the school. When importing or connecting to an existing database, only the login name as stored in the existing database should be transferred to the online learning platform (unidirectional information flow). The password must meet the guidelines as specified in section 9.1 and may therefore have to be reassigned. The school or the school supervising authority determines the procedure in form of a set of user rules.

9.4 Public Areas

It is basically possible to make certain areas of an online learning platform publicly accessible. The same data protection regulations apply to these areas as to other school websites, in particular with regard to the naming or depiction of learners or teachers; in addition, the Telemedia Act and the Telecommunications Act apply. In compliance with the relevant regulations, general accessibility must always be avoided as soon as personal data becomes visible as a result.

9.5 Search Engines

Areas in which user-specific data is stored may not be offered publicly. It must be ensured that public search engines (Google, Bing, etc.) do not have access to these areas.

9.6 Role Concept

The following roles are usually predefined in an online learning platform:

- *Administrator:* The administrator has all permissions for all areas and content, he can change user account settings and change system-wide settings.
- *Course Manager:* The course administrator can create areas and assign authorizations. This privilege can be limited to sub-areas (course categories, training courses, subjects, grades).
- *Teacher:* Teachers can maintain contents in certain areas, admit participants, view learning progress and learning outcomes.
- *Participant:* Participants can work in the areas to which they have access rights, use learning content and make entries.

Further roles can be defined in accordance with the school's role and authorization concept.

The following principles must be observed when assigning rights and roles:
An administrator can access all areas. Persons with administration rights can therefore view all courses as well as contributions from learners and teachers; this also includes evaluations. Special care must therefore be taken when authorizing administrators, namely:

- Each administrator must be assigned an individual personal user account, i.e. it is not permitted for several administrators to use the same user account (group administrator account). The administrator's login name must be pseudonymous to prevent misuse of the account. The pseudonym must be chosen in such a way that it is not easily identified.

- Administrators who also perform other activities within the online learning platform, such as teaching tasks, must have a separate user account for this purpose. It must therefore be possible to assign several user accounts to a person according to their different roles.
- The number of administrator accounts must be kept as low as possible in order to minimize the risk of misuse (e.g. unauthorized access, uncontrollable assignment of rights, etc.). However, a substitute arrangement must be guaranteed.
- Administrator rights may only be granted to those who actually have to perform corresponding tasks within the system.
- All activities of administrators should be logged solely for the purposes of data protection control for a period of typically at least six months and no more than one year. The logs should be checked regularly according to the principle of dual control.

9.7 Access Privileges

9.7.1 Access by School Internal Departments or Persons

The rights of access to the system for teachers, students, school management and administrators must be defined in advance in writing in a role and authorization concept. Among other things, personnel substitution regulations must also be observed. Members of the school management and, if necessary, officials have the right to observe lessons. This right serves to fulfil the management task, to obtain information and impressions on the development of teaching and school concepts. In many schools, exams are presented to the school management for information and consideration after evaluation and before being returned to the students. Nevertheless, such actions may only take place to the extent necessary for the respective task.

If online learning platforms are used, they automatically become part of the teaching work. This means that the agreements made within the school with regard to observations also apply to online learning platforms.

The way in which the school management inspects the work with an online learning platform must correspond to the internal school agreements, as they apply to classroom observations. Users of the online learning platform must be informed about this procedure and agreements before the commencement of such usage. Each inspection is documented in the same way as is required and specified for observations in regular classroom work. Monitoring of the work with the online learning platform by the school management or other departments and persons is not permitted. In particular, the activities of learners must not be monitored by teachers. The same applies if the online learning platform is used for pedagogical tasks such as organized chats on specific topics and group work where both of which are subject to grading. In this case, the teacher may monitor the activity that is necessary for the grading. The scope of the data that should be visible to teachers must therefore be pedagogically justified and determined by the school conference. Similarly, the activities of teachers on the online learning platform must not be monitored by superiors. The corresponding regulations are to be laid down in the user regulations.

9.7.2 Granting Access to Data by School External Parties or Persons

In principle, school outsiders have no access to protected areas of the online learning platform. If it is necessary in justified exceptional cases, every access of this kind must first be checked by the person responsible for its legality. Participants must be informed in a timely manner about external access to data on the online learning platform. Within the framework of data protection regulations, permitted external persons who are not active as teachers, learners or employees in the school administration may also have temporary and limited access to protected areas of the online learning platform if this is necessary to guarantee the function of the system, e.g. for remote maintenance. In such cases, a contract for order processing must be concluded with the respective external order processor.

9.8 Data Deletion

If the storage of personal data requires consent, the stored data of teachers and learners will be deleted if the consent is withdrawn. The data of learners in courses (last editing, lessons completed, errors, correction notes, etc.) are deleted at the end of the current school year. Retention periods from the state school laws and related legal regulations must also be observed. It must be specified in writing how the retention periods are to be complied with. Exceptions are permitted, for example, for projects spanning several school years in preparation for follow-up examinations, for courses relevant to the final examination and on account of the school's documentation requirements. Students' e-portfolios can also be stored as a back-up copy during the entire period of their school attendance. The remaining data of learners and teachers will be deleted at the end of the school year in which the teacher has left school or the learner has left school.

User accounts of learners and teachers must be deleted after they have left the school, or if they withdraw their consent.

The log data mentioned in section 6.1.3 (e.g. when a user accessed which data, or when functions were used) accumulate on the server side and make it possible to investigate and solve problems during technical operation and user access if necessary. The storage period should not exceed ten days. A longer storage period is only permitted in justified exceptional cases. For further regulations on logging, please refer to the orientation guide *Protokollierung* (Logging) mentioned already in section 6.1.3.

The corresponding regulations must be specified in the respective user regulations.

9.9 Separation of Databases

Each school is regarded as an independent organizational unit. The data of different schools must be kept and managed logically separate from each other. It must at least be guaranteed that schools can only access their own data. For this purpose, reference is made to the OH Mandantenfähigkeit (Guidebook for Multi-Client Capability) from the working group Technische und organisatorische Datenschutzfragen (Technical and Organisational Data Protection Issues) of the Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Conference of the Independent Data Protection Authorities of the Federal Government and the States of Germany) in the current version.

9.10 Further Technical Measurements

Concrete measures should be proposed which in particular prevent access to the data from outside the school and ensure that data transmission to the teachers' and learners' home computers and, depending on the role concept, to parents' computers is secure against unauthorized access. The measures to be taken depend on the concrete circumstances of the individual case. The level of security required varies depending on the type of data concerned, the group of persons who are intended to have access to it, and the location in which the data is stored. If it is merely an online learning platform that only provides information for learners, the same high level of protection is not required compared to an online learning platform on which grades are stored and to which third parties have access to certain areas.

These security measures concern three aspects in particular: the data security on the server, the protection of the administrator's access and the protection of data transmission to the user.

- For the use of the online learning platform, a comprehensive rights and role concept must be provided on the server, which only allows each user access to only those program areas for which they are intended to.
- Administrator access is a very critical issue within the online learning platform. The password should comply with common security precautions. Please refer to the current basic IT protection catalogues for creating passwords as mentioned in section 9.1. In view of the often experimental nature of learners, administration should only take place via computers that are inaccessible to students, as this reduces the risk of learners installing malware unnoticed on computers used for administration which could then gain access to the administrator password. Furthermore, the use of a good firewall and up-to-date anti-virus software on the server is absolutely essential. A two-factor authentication, as it is standard for many web-based applications, will be indispensable for administrative access to applications with increased functionality, depending on the result of the data protection impact assessment. The same precaution procedure is applicable to the roles of course manager and teacher (see Section 9.6).
- The data transmission between server and user of an online learning platform must be encrypted. Depending on the respective online learning platform, the use of the encryption technology has to be examined individually for this purpose.