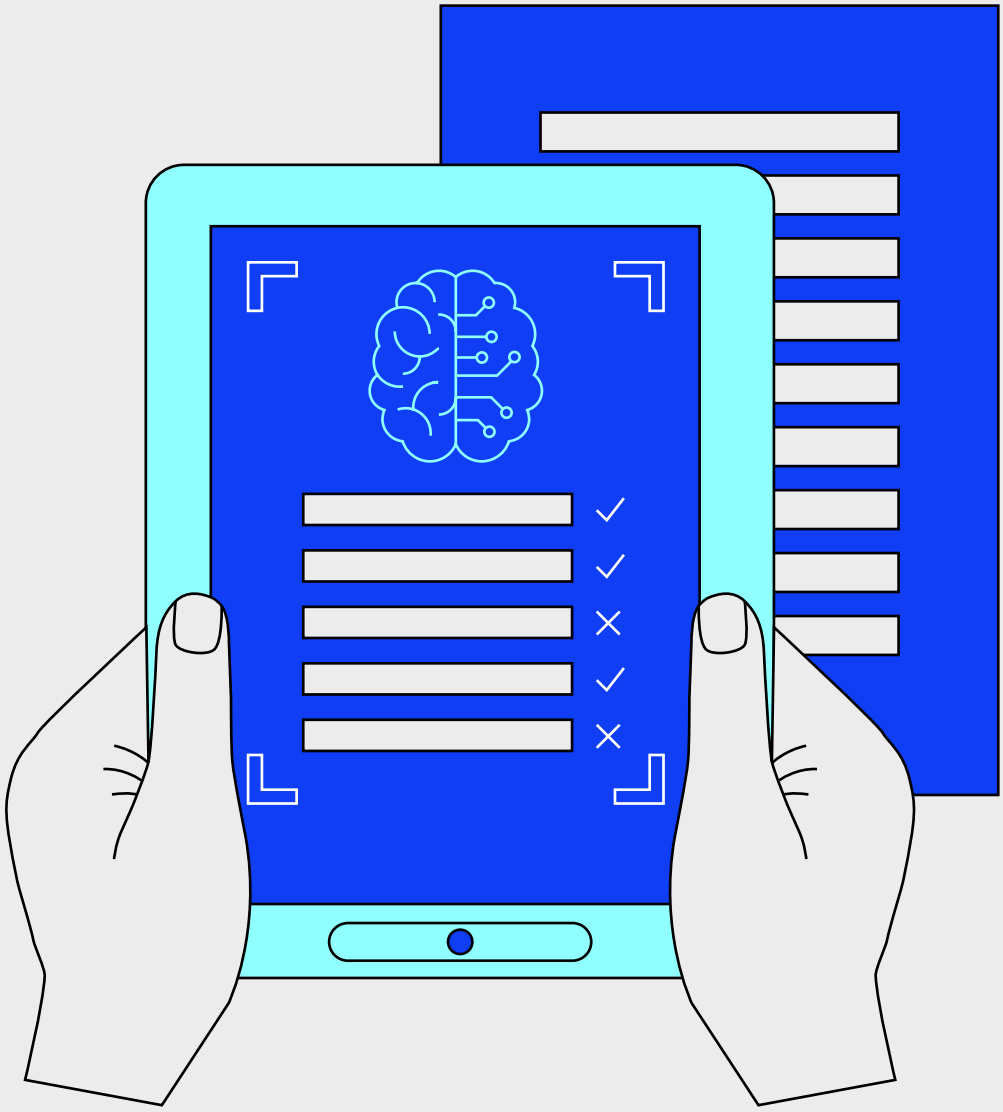
Innovation Sandbox for
Artificial Intelligence



Artificial Intelligence in Education

Legal Best Practices

metropolitan konferenz zürich

Kanton Zürich

Innovation Zurich

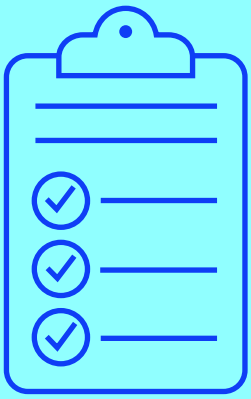
Artificial Intelligence (AI) offers great potential within education. AI applications enable individualised learning and can provide support to teachers by reducing the burden of repetitive tasks such as correction work. However, there are also various regulatory and ethical challenges. While AI-supported tools are already in use in schools, the legal framework is often insufficiently clear to AI solution providers, teachers and school officials. The present guidelines provide an overview of legal aspects such as data protection and copyright, for when implementing AI applications. This document was drawn up based on a specific use case during which school pupils used a smartphone scan to automatically correct their handwritten math work and spelling exercises. Whereas these guidelines are based on the legal framework of a state school in the Canton of Zurich, the legal situation is similar in other cantons. The relevant regulations are, however, applied differently from canton to canton. While primarily directed at AI solution providers, these guidelines may also offer helpful insights to school officials as well.

Innovation Sandbox for Artificial Intelligence (AI)

This document was created within the scope of the Innovation Sandbox for Artificial Intelligence (AI). The sandbox is a test environment for the implementation of AI projects from various sectors. This broad-based initiative involving public administration, industry and research, is designed to promote responsible innovation by allowing the project team and participating organisations to collaborate closely on regulatory questions and enabling the use of novel data sources.
More Information

I.

Preparing an AI project



1. Identifying the legal areas concerned

From a legal perspective, the first step involves identifying the legal areas concerned. In most cases, **data protection law** is likely to play a major role; however, depending on the AI application concerned, other areas of law may also be relevant, e.g. **copyright law**, areas of **administrative law (especially school law)**, but also general **contract law**, i.e. when clarifying the relationship between the provider of the AI tool and the respective school.

Ideally, identifying the legal areas concerned will be done jointly by the provider of the AI tool and the persons involved on the part of the school. The parties involved may find it worthwhile to consult a cantonal office, e.g. the Department of Education as the body responsible for digitisation topics.

2. Identifying the relevant legal bases

Once the legal areas concerned have been determined, the next step is to identify the applicable legal bases. This can present a bit of a challenge, especially in the domain of data protection. Data processing by private persons and by federal authorities is subject to the **Federal Act on Data Protection (FADP)**, with different regulations within FADP being applied for various entities. Private providers of AI tools must adhere to the relevant regulations of FADP for their own data processing. The same applies when private providers offer AI tools to private persons or to a federal authority.

Elementary schools (Volksschulen) are cantonal public bodies. Cantonal and municipal data processing is subject to cantonal rules and regulations which, in the Canton of Zurich, is the law governing information and data protection **[Gesetz über die Information und den Datenschutz (IDG)]**. Schools in the Canton of Zurich must be compliant with this law. In addition, municipal-level decrees, such as municipal laws, or education-specific decrees, such as the law governing elementary schools (Volksschulgesetz), also apply. Some schools or educational institutions also have internal directives that need to be followed. The schools are responsible for ensuring that third parties used to help fulfil their public duties also comply with the rules and regulations that apply to them. For AI providers, this means that they must be able to adhere to the, in part, strict stipulations that apply to data processing by public institutions. For example, a public body may have special rules in place for use of cloud services.

«Due to the legal complexity of AI projects in schools, a holistic approach is recommended.»

Dr. Stephanie Volz, ITSL University of Zurich

3. Involving the institutions concerned

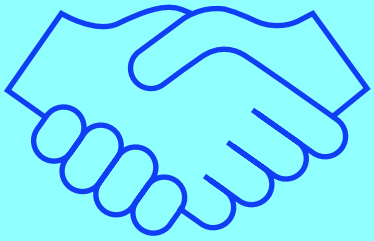
Providers of AI tools wishing to collaborate with schools will often seek to contact teachers. Although teachers are the key to the classroom, so to

speak, involvement of other persons or institutions should not be neglected. Possible other persons or institutions are: school management or a school's ICT or digitisation officer. Depending on the size and risk level of the project, it makes sense to contact the competent department of education first. Furthermore, depending on the type of endeavour, involvement of the cantonal data protection authorities is also recommended.

Involvement of various bodies and institutions allows for projects to be broadly supported and for potential problems to be recognised and addressed early on. These are crucial factors for the success of a project.

II.

Project implementation



1. Clarifying liability and responsibility

Responsibility and liability are further important points that need to be clarified by the parties involved. To that end, the first step is to clarify competences ("Who is permitted to do what?"); based on this, roles need to be defined and tasks or, that is to say, the respective rights and obligations distributed among the parties. All parties involved must also dedicate careful thought to how best to minimise any risks.

It is very important to clarify responsibilities and impose obligations under data protection law (cp. III.2.). This will also involve clarifying any questions of potential liability in the event of damage occurring. From a data protection viewpoint, liability situations often result from cantonal regulations. Schools as public sector bodies generally remain liable even if and when data processing is carried out by a third party. However, the schools will (need to) impose certain obligations by contract on the AI tool providers which must be adhered to when processing personal data. AI providers who fail to observe these obligations will become liable to the respective public body.

2. Identifying the relevant legal bases

Processing of personal data by a public body such as a school is only permissible if there is a legitimate basis **(principle of lawfulness)**. Therefore, the most important step prior to data processing by a school is to identify the applicable legal basis. As a rule, this information can be found in the law governing the respective areas – i.e., in the case of schools, in the relevant laws governing elementary schools (Volksschulgesetze) or in decrees based on these laws. A legal basis can be a law or an ordinance.

«Clarified framework conditions are a necessary prerequisite for trustworthy AI in education.»

Nelly Buchser, Educa

Most laws governing elementary schools (Volksschulgesetze) include legal bases for a number of data processing operations. Furthermore, the school districts or individual schools may also have certain legal bases of their own. Clarification as to which are relevant and whether they will also be sufficient in the specific case of AI tool use needs to be sought on a case-by-case basis. In many instances, the statutory bases that cover data processing for the purpose of fulfilling a school's educational mission are also likely to cover use of AI tools as well.

III.

Data protection implications

1. Handling of personal data

The (federal or cantonal) data protection laws apply when personal data is processed. **Personal data** means any information relating to an **identified or identifiable natural person.** A natural person is identifiable if their identity can be determined directly from the data itself or from the context in combination with further data, to the extent that establishing the identity does not require a disproportionate effort. Identifiability is relative, i.e. a natural person can be identifiable to someone who has additional knowledge, but not to someone else.

Using handwritten data as an example, handwritten worksheets would often qualify as personal data for teachers because teachers are usually able to identify their pupils based on their handwriting. Clarification as to whether personal data is, then, also available to the provider of an AI tool needs to be sought on a case-by-case basis: if the AI provider only receives the handwritten worksheets without any further identifiable characteristics (e.g. the name) from which the provider could make a connection to a specific person, this does not qualify as personal data. If, by contrast, a worksheet contains identifiable characteristics, e.g. because it includes a name, then this qualifies as personal data. When it qualifies as personal data, the relevant data protection laws apply, and processing must be in keeping with the requirements stipulated therein. When developing an AI tool, the goal from the outset should therefore be to avoid creating any personal data, or as little as possible. Having said that, since only very few clues or indicators are needed for a reference to be made to a specific person, creation of personal data is often inevitable.

2. Clarifying the data protection situation

A crucial question from a data protection perspective is that of responsibility under data protection law. Responsibility resides with the person who–alone or with others–decides on the purpose and means of data processing. In principle, this person is responsible for data protection compliance.
From a data protection law perspective, if a state school uses AI tools to perform its tasks and personal data is processed when doing so, this constellation is to be qualified as outsourcing or as data processing by order. The school's data processing is carried out together with or by a third party. However, the responsibility for data processing remains with the school. Therefore, the same law applies to the data processing party as to the public body that outsourced the data processing. In the Canton of Zurich, the Data Protection Act [Gesetz über die Information und den Datenschutz (IDG)] is the law applicable for Zurich's state schools and the Federal Data Protection Act (FDAP) for private schools.

The public body must assume its responsibility in different ways, one being to contractually involve the third party/ies in the responsibility. This is achieved through concluding a contract which by law must meet certain minimum requirements in relation to content. In the Canton of Zurich, the relevant provisions can be found e.g. in the cantonal data protection ordinance [Verordnung über die Information und den Datenschutz] included in the GTC of the Zurich Government Council regarding IT services. However, equivalent provisions may also be negotiated on an individual basis.

3. Observing the relevant data protection principles

Data protection is one of the most important topics in the context of implementing digital solutions in schools. In order for a project to be data protection compliant, the **data protection principles** must be observed. Compliance with data protection principles must be ensured at every stage of a project. It is important to implement these principles already in the development stage of a project (Privacy by Design). Furthermore, any default settings should be designed in a data protection friendly manner, i.e. in order for as little data as possible to be processed (Privacy by Default). The data protection principles can be found in similar form in both the FDAP and the cantonal data protection laws.

In addition to the previously mentioned principle of **lawfulness/legality** by which data processing by state bodies such as schools (cp. II.2.) requires a **legal basis,** there are several other principles which must also be adhered to.
The principle of **proportionality** is an essential one. Data processing must be adequate and necessary for achieving a desired goal, i.e. data processing is to be limited to the minimum necessary.

«The collection of personal data that is not strictly necessary for an AI application significantly increases legal complexity.»

Dr. Stephanie Volz, ITSL University of Zurich

For instance, specification of an exact date of birth when registering for an AI tool is usually unnecessary. Furthermore, use of a tool without any prior registration (known as guest access) helps to ensure proportionality. Registration as well as allocation of teaching content and automated corrections could be done via a QR code, for instance. This principle is complemented by the principle of data minimisation, according to which personal data that is no longer needed for the processing purpose is destroyed or rendered anonymous. This also means that the data may only be stored with the teacher and the AI tool provider for as long as necessary.

In accordance with the principle of **purpose limitation**, data may only be processed for the purpose for which it was collected. This purpose must be such that the data subject can **recognise** it. As well as the purpose, data processing in itself must also be recognisable. When data is processed by a public body, transparency often arises from the statutory basis **(principle of transparency)**. With a view to ensuring transparency, data protection laws stipulate fairly extensive **duties to provide information for processors** of personal data.

Any breach of a data processing principle renders the data processing unlawful. A justification is required in order for data processing to be carried out.

4. Compliance with the duty to provide information

The FDAP as well as cantonal data processing laws, e.g. IDG, oblige data controllers, i.e. the schools, to inform the data subjects about the data processing. The FDAP requires that the following information be provided as a minimum: the data processing entity's identity and contact details, the purpose of processing and any recipients or categories of recipients to whom/which personal data is disclosed. Pursuant to IDG, information is additionally to be provided on the procured data and the legal basis for data processing. Although compliance with the duty to provide information rests with the schools as the data controllers, the providers of the respective AI tool will generally need to assist with the specific implementation.

5. Ensuring data and information security

Generally speaking, unauthorised data access poses a big risk to personal data. This is why data controllers are under the obligation to ensure that data processing is designed, both technically and organisationally, in such a way that the data protection principles are adhered to and data security

appropriate to the risk is ensured through appropriate technical and organisational measures. The measures to be taken must be based on the state of the art, the nature and the scope of the data processing, as well as the risk posed by the processing.

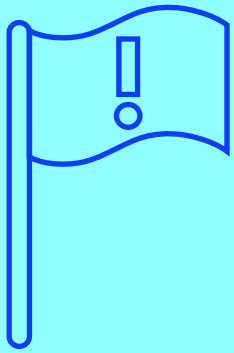
When designing an AI tool, care should be taken to generate as little personal data as possible, e.g. through avoiding use of personal data in the registration process (cp. III.3.). Another example: to make sure pupils do not accidentally upload personal documents such as bank statements or health records instead of worksheets, technical precautions can be taken to ensure that an upload is only possible once a worksheet has been recognised.

6. Implementing a Data Protection Impact Assessment (DPIA)

Prior to an envisaged new data processing activity, public sector bodies in the Canton of Zurich, and thus also schools, must carry out a **Data Protection Impact Assessment (DPIA)** to assess the risks to compliance with the fundamental rights of the data subjects. The implementation of digitisation projects and use of new technologies qualify as new data processing acts and require a prior DPIA. If the DPIA shows that there are particular risks to compliance of the fundamental rights of the data subjects, the envisaged processing of personal data must be submitted to the cantonal data protection officer for review (prior checking). Projects with use of AI employ new technologies that involve particular risks to the fundamental rights of the data subjects and must, on all accounts, be submitted to the data protection officer for **prior checking**. Within the scope of prior checking, the data protection officers look into whether the envisaged project can be implemented in compliance with data protection requirements, or whether adjustments need to be made. Prior checking requires that various documents be submitted to the data protection officers. These include an ISDP concept, the DPIA and the legal basis analysis. Submission of the DPIA is the responsibility of the school. However, to ensure that the DPIA is carried out correctly, the AI tool providers must supply the school with certain information about the AI tool being offered.

IV.

Points of particular interest



1. Caution when processing personal data of children

When AI tools are used in schools, data processing will generally concern data in relation to children (e.g. learning progress). That notwithstanding, careful consideration must be given to the particular risk when processing data, e.g. within the scope of the DPIA (cp. III.6.).

The particular circumstances involved when processing data of children must also be borne in mind when checking whether the principle of proportionality has been taken into account. In addition, the duty to provide information and be transparent vis-à-vis children must also be exercised vis-à-vis the children's parents, which means that the children's legal guardians must be informed about any data processing. If a data processing activity requires consent, this consent needs to be obtained from the legal guardian/s (cp. IV.5.). These duties are generally the responsibility of the respective school; however, the AI tool provider/s will also need to supply certain information to the school.

2. Caution when processing sensitive data or profiling

Both federal and cantonal data protection laws differentiate between two categories of personal data: in addition to "normal" personal data, there is what is known as "sensitive" personal data, the processing of which is subject to special requirements.

Pursuant to federal law (and as similarly stipulated in Zurich's cantonal law), data relating to religious, philosophical, political or trade union-related views or activities, data relating to health, the private sphere or affiliation to a race or ethnicity, genetic data, biometric data that unequivocally identifies a natural person, data relating to administrative and criminal proceedings or sanctions, as well as data relating to social security measures, all qualify as sensitive personal data. In the domain of schools it may be the case that sensitive personal data is processed, possible examples being, in particular, health-related data (e.g. educationally relevant diagnoses such as notes on dyslexia or dyscalculia), information related to religion or, in individual cases, biometric data. In this context it is important to note that biometric data only qualifies as sensitive data if it is data in relation to physical, physiological or behavioural characteristics of a natural person obtained through specific technical processing which allow for the unequivocal identification of the data subject or which confirm an existing identification. AI tools may process biometrical data, for instance when it is based on a technical analysis of handwriting or voice recognition.

Special rules also apply if information is compiled in a way that permits the evaluation of substantial personal aspects of natural persons. This is referred to as profiling which also falls within the remit of sensitive personal data.

Processing of sensitive personal data or profiling requires a statutory basis in a formal law, i.e., the law must have been passed by the competent parliament – cantonal or municipal parliament. Zurich's law governing elementary education (Zürcherisches Volksschulgesetz) contains various statutory bases for data processing in schools and is a formal law; this means that, in certain cases, it can provide the statutory basis for processing sensitive person-

al data, provided it contains a sufficiently specific provision for such data processing.

3. Caution with use of (personal) data for own purposes

Providers of AI tools often have an interest in using data generated during use for their own purposes. For instance, data generated from corrections can be useful to further train the AI tool or for further development of the service provided.

From a data protection perspective, if the data in the respective school comes in anonymised form and, thus, no more personal data is available, disclosure of the data is permissible. However, rendering the (personal) data anonymous is, in itself, to be qualified as data processing.

If (personal) data collected in a school is to be used for another purpose than the one for which it was originally collected, this qualifies as a change of purpose from a data protection law perspective, which requires a legal basis. This means that use of the correction data for training and further development purposes would require a separate statutory basis which is usually unavailable.

In theory, the Canton of Zurich offers two options to use the data nonetheless: disclosure of personal data to third parties is permitted if **consent has been given for the individual case**. In order for personal data of school pupils to be disclosed, the consent of the pupils concerned and/or their legal guardians would need to be obtained. Whether and to what extent this provision can be applied in a specific situation will need to be clarified for each individual case.

A further option presents itself if **data processing is not related to specific persons**. Most data protection laws allow public bodies to disclose data for purposes not related to specific persons, e.g. data for research, planning or statistical purposes. A prerequisite for this is the prior anonymisation of the data concerned and that no inferences about the data subjects can be drawn from the evaluations. Training and further development of AI tools may be considered for purposes not related to specific persons. However, here too, prior clarification is needed as to whether this option can be resorted to in a specific individual case, given that interpretation of the relevant provisions varies considerably from canton to canton.

Furthermore, besides data protection, there may be copyright law issues to consider as well. So far, it is unclear as to whether use of copyrighted works for AI tool training presents an act relevant to copyright law and, if so, whether invocation of the data mining exception as set forth in Art. 24d of the Federal Act on Copyright and Related Rights [Urheberrechtsgesetz (UrG)] is permissible. Pursuant to the said provision, the reproduction of copyrighted works for scientific purposes is permissible under certain conditions. In principle, the provision also applies to commercial purposes and, thus, could be applied to AI tool training as well. However the legal situation is disputed, which is why in-depth legal clarification is strongly suggested for each individual case.

4. Caution with use of teaching material

When an AI tool uses photographs, texts or similar from existing teaching material, copyright law must also be observed. Digitisation of teaching material qualifies as a reproduction act relevant under copyright law which, in principle, requires consent from the author. Whereas Swiss copyright law provides for an exception to use of copyrighted works in the classroom for educational purposes, application thereof is restricted to use of the works in the classroom itself. Commercial exploitation of the works is not affected by this. As a rule, the providers of AI tools pursue their own commercial goals, which is why the restriction is unlikely to apply. If a provider of an AI tool wishes to use existing teaching material, the prior consent of the author would need to be obtained.

5. Caution when embedding large language models

Providers of AI tools have the option of embedding large language models (LLM) into their own AI tool via an interface (API). However, from a legal perspective, caution is advised when embedding such third-party tools. In terms of data protection law,

attention should be paid to ensure that there can be no flow of personal data, neither intentional nor unintentional, to the LLM provider. Data security is another area that needs to be considered. Furthermore, copyright law issues can arise if an LLM provider unlawfully uses content that is protected by copyright for his/her model and this infringing content appears in the AI tool.

«The integration of Large Language Models offers great opportunities for solution providers, but also leads to legal risks that are difficult to control.»

Raphael von Thiessen, Head of Innovation Sandbox for AI

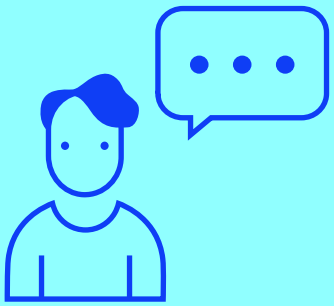
6. Less relevant - consent

In very few cases, data processing will require consent. Such consent may, in isolated cases, serve to justify an otherwise inadmissible data processing act. In certain cases, if there is no (sufficient) statutory basis or if data is to be used for a purpose other than the one for which it was originally collected, state bodies can obtain consent from the data subjects concerned. However, obtaining such consent is on a case-by-case basis. In the case of private persons, besides consent, satisfying overriding private or public interests is also seen as a justification reason. This also includes processing of data not related to specific persons for research purposes. This reason could, for instance, apply to the use of data for training and testing an AI tool. However, the legal situation in this respect is disputed.

It can be said, therefore, that obtaining consent is likely only necessary in very few cases. Moreover, seeing that obtaining consent is contingent on various conditions, e.g. consent must be given voluntarily which implies a real choice by the data subject, taking the route of consent as a basis for data processing is often not recommended.

V.

Recommendations of the AI Innovation Sandbox team



The fast-paced development of AI in the educational sector offers considerable potential but also involves major challenges, particularly in relation to legal and ethical questions. There is an urgent need for clear guidelines and in-depth interdisciplinary dialogue so as to ensure that AI is integrated responsibly and effectively in the educational system. The AI Innovation Sandbox team has compiled the following recommendations based on the current situation and with a view to collectively shaping the future of AI in education:

Uniform strategy for legal security

The regulatory framework currently varies from canton to canton in Switzerland. A uniform, nationwide strategy and set of regulations would contribute to legal security and consistency in the handling of AI applications and tools. This would create a clear and comprehensible basis for the integration and use of AI technologies in schools and, thus, facilitate use of these technologies across Switzerland.

Cantonal or regional contact points for AI providers

It would be very helpful to establish cantonal or regional contact points where AI providers can have their products checked as to compliance with data protection. This would contribute to preventing repetitions and duplications by saving individual schools from having to clarify the same questions with various providers. Furthermore, these points of contact could operate as important interfaces between theory and practice in order to overcome currently existing discrepancies.

Pursuit of own goals when developing AI products

There is considerable uncertainty regarding reuse of data and copyrighted works for the development of AI solutions. Therefore, more in-depth political and societal discussions are needed to clarify to what extent manufacturers should be permitted to use personal data and protected works for innovative developments in the educational sphere, for their own purposes and for commercial activities. In this regard, particular attention should be paid to finding a balance between promoting innovation and protecting personal and intellectual property rights.

The intention of these recommendations is to contribute to the development of a comprehensive and future-proof strategy for use of AI in the educational sector in Switzerland. They form the basis for a broad and in-depth dialogue between all stakeholders, in order to harmonise the topic of AI in the educational sector and to approach the subject in a constructive manner.

Individuals and organisations involved in this report

Expert interviews

René Moser, Office of Elementary Education (Volksschulamt), Canton of Zurich
Nelly Buchser, Educa
Karen Grossmann, Educa
Manuel Brogli, Kellerhals Carrard
Verena Rohrer, Swiss EdTech Collider
Carmen Sieber, Swiss EdTech Collider
Moria Zürrer, School principal & president of Schule Medien Informatik Zurich

Authors

Dr. iur. Stephanie Volz,
Regulatory Expert Innovation Sandbox for AI, ITSL University of Zurich

Raphael von Thiessen,
Head of Innovation Sandbox for AI, Division of Business and Economic Development, Canton of Zurich

Case study provided by the Innovation Sandbox for Artificial Intelligence (AI)

The company Herby Vision AG served as a case study within the Sandbox. The said company submitted a project proposal to the Sandbox in the spring of 2022. Herby Vision AG offers automated corrections of primary school homework and assignments by way of reviewing handwritten learning content through AI-based image recognition. Thanks to the Testbed program provided by the Swiss EdTech Collider, Herby Vision AG was able to test its offering in various schools. The content of the present guidelines was devised between July 2022 and September 2023 based on the specific implementation of Herby Vision AG.

Imprint

Publisher
Division of Business and Economic Development, Canton of Zurich
Metropolitan Area Zurich Association
Innovation Zurich

Project conception and coordination
Raphael von Thiessen
Location Promotion Canton of Zurich
8090 Zurich
raphael.vonthiessen@vd.zh.ch

Concept in collaboration with:
Stephanie Volz
Isabell Metzler
Patrick Arnecke

Authors
Dr. iur. Stephanie Volz
Raphael von Thiessen

Design
Sibylle Brodbeck, sibyllebrodbeck.ch

Publication
This report is published exclusively in digital format and in the languages German and English

Translation
Mila Myrsep, Word for Word Ltd. Liab. Co.

Project Steering
Division of Business and Economic Development, Canton of Zurich
Statistical Office, Canton of Zurich
Division of Digital Government, Chancellery, Canton of Zurich
Office for Economy, Canton of Schwyz
Metropolitan Area Zurich Association
ETH AI Center
Center for Information Technology, Society, and Law (ITSL) University of Zurich