RESOLUTION ON E-LEARNING PLATFORMS

40th International Conference of Data Protection and Privacy Commissioners
Tuesday 23rd October 2018, Brussels

CO-AUTHORS:

- Office of the Information and Privacy Commissioner, Alberta, Canada
- Office of the Information and Privacy Commissioner, Ontario, Canada
- Office of the Privacy Commissioner of Canada
- Office for Personal Data Protection, Czech Republic
- Commission Nationale de l'Informatique et des Libertés, France
- National Commission for the Control and Protection of Personal Data, Morocco

CO-SPONSORS:

- Thüringer Landesbeauftragte für den Datenschutz, Thuringia, Germany
- Privacy Commissioner for Personal Data, Hong Kong
- Garante per la protezione dei dati personali, Italy
- Data Protection Registrar, Jersey
- National Privacy Commissioner, Philippines
- Personal Data Protection Office, Poland
- [Agencia española de protección de datos, Spain]

A global marketplace of e-learning platforms has emerged to help education authorities provide enhanced educational services and improve outcomes for children and youth. A growing number of educational authorities are using these platforms to support the delivery of education in the classroom, and to gain a better understanding of student learning needs.

Some of these e-learning platforms and the learning analytics they facilitate have enormous capacity to foster the development of innovative and effective learning practices. At their best, they can enhance and complement the interactions of students, parents and educators in the educational environment and help them fulfil their respective potential. Nevertheless, e-learning platforms may pose threats to privacy arising from the collection, use, reuse, disclosure and storage of the personal data of these individuals.

The personal data of children and youth merit specific protection and should be processed only on the basis of sufficient legal ground. Children and youth are entitled to have their privacy protected and must be able to exercise their data protection rights with the support of their parents or guardians. Parents have to be able to assist their children and participate actively in the exercise of these rights.

Classrooms have become increasingly networked environments that may put the privacy of children at risk. Specifically, these connected classrooms raise issues of transparency, in view of the fact that inappropriate data processing practices by e-learning platforms, opaque automated decision-making and misuse of learning analytics risk undermining data protection and privacy rights. In the case of children and youth, this can have significant and long-term social, economic and professional consequences, and fail to account for their evolving capacities.

Based on the above, and in keeping with the objective of adopting resolutions on subjects of common interest or concern, the 40th International Conference of Data Protection and Privacy Commissioners (ICDPPC) calls upon all relevant parties in the field of e-learning, and particularly

- E-learning platform providers and manufacturers, including providers of data driven services directed at students; and

- Educational authorities, including ministries of education, school boards, school administrators and educators

to fully respect students', parents' and educators' ("individuals") rights to the protection of their personal data and privacy, and to guarantee that the data collected is solely used for educational purposes in compliance with data protection law.

Parties are urged to take the recommended actions below at every stage of the development, implementation and use of e-learning platforms.

1) Educational authorities are called upon to:

a) **Ensure they have authority and expertise to engage the services of e-learning platforms**. There should be a clear internal allocation of roles, responsibilities and delineation of authority between educators, school administrators and other relevant educational authorities to be able to establish legal authority and accountability when dealing and contracting with providers of e-learning platforms. The authorized representatives should have a clear understanding of applicable data protection and privacy laws to guarantee its inclusion in the terms and provisions of the contracts and third party agreements.

b) **Develop policies and procedures to evaluate, approve and support the use of e-learning platforms and, where feasible or required, conduct data protection/privacy impact assessments**. These policies should promote individual control over personal data, clarify the roles and responsibilities among the various actors involved in e-learning platforms, mitigate risks and promote accountability.

c) **Provide training and on-going support for educators.** Educators must be equipped with up-to-date, relevant and sufficient information on data protection and privacy rights to be able to implement effective e-learning platforms. Access to resources, trainings and workshops enable educators to maximize the benefits of e-learning platforms and to then provide effective guidance and support to students and parents on proper use.

d) **Work with other educational authorities and, in cooperation with local data protection authorities, to agree on common standards for engaging e-learning platforms**. This collaborative approach towards commonly accepted practices increases leverage, knowledge exchange, best practice development, and resource maximisation in order to overcome any inconsistent privacy and security practice in the delivery of e-learning platform services.

e) **Where required or appropriate, seek valid, informed and meaningful consent from individuals.** The legal basis for the processing of student data by an e-learning platform commissioned by an educational institution should be determined by law or rules established by competent regulatory authorities, wherever available. If no such legal basis is available, parental consent, student consent or both, as appropriate, must be obtained. The validity of this consent presumes that its withholding leads to no disadvantage of the student compared to their consenting peers. The decision, at any time, to opt out or withdraw consent should allow individuals to opt out of all or some of the data processing, if practical.

f) **Consistent with domestic law, implement a policy for individuals who access the e-learning platform with their personal electronic devices.** This policy should clarify appropriate uses of the e-learning platform and any consequences of using a personal device – especially when installing software or mobile applications.

2) ***Educational authorities and e-learning platform providers and manufacturers are called upon to, jointly or independently according to domestic data protection law:***

a) **Ensure that e-learning platforms appropriately safeguard users' personal data and meet the appropriate data protection standards**. However the use of e-learning platforms is governed, the provisions must always be consistent with applicable data protection laws and requirements.

b) **Make sure that the purposes for which personal data are being collected, processed and used are legitimate, suited to the context and authorized by law.** All collection of student

data should be limited to what is needed for educational purposes. By default, no other use of this data should take place, including for commercial or marketing purposes. Student data must never be repurposed or used for non-educational purposes without freely given express consent, unless there is legislation allowing for re-purposing. Secondary processing should proceed with de-identified data whenever possible, including for statistical and research purposes.

c) **Minimise the amount of personal data to be processed**. The collection, use, retention and disclosure of personal data, and particularly student data, should always be limited to what is necessary to fulfil authorized purposes. Reducing the risk posed by the excessive collection of student data should be a core principle to guide data processing practices of e-learning platforms.

d) **Before collecting personal data, notify individuals about the personal data to be processed by the e-learning platform and the reasons for processing.** The notice should be provided in a timely, age-appropriate, clear and concise fashion. Graphics, audio, video or other media may be used in addition to textual information. More detailed information should be easily accessible. The notice needs to enable individuals to make informed decisions. Further, notices should explain uses and disclosures to third parties, the risks of harm arising from processing personal data, a summary of protections and assurances in place, and an account of existing privacy rights and options available.

e) **As far as possible, allow individuals to use the e-learning platform with de-identified data.** To avoid the excessive collection of personal data, individuals should be able to use the e-learning platforms anonymously or with unlinkable pseudonyms.

f) **As far as possible, avoid the use of personal data per se, and particularly data on learning behaviour, for predictive purposes, profiling or automated decision-making.** The use of students' personal data to make subjective assessments or generate assumptions has the potential to undermine the evolving capacities of children and youth. Where the data is used for statistical analysis and profiling, for making subjective assessments, for predicting behaviour or as part of a decision-making process it should

be clearly communicated to students and parents. They should be provided with mechanisms to challenge these assessments.

g) **Embed and employ tools that enable individuals to control their personal data and effectively exercise their privacy rights, including their right to access, correction, erasure and, where applicable, data portability.** These rights over personal data should be extended to any metadata, inferences, assessments, and profiles compiled about students, parents and educators.

h) **Set and respect retention periods for different categories of personal data.** Retain data and metadata only as long as required to satisfy the purposes of collection and their intended use. In particular, logs of interactions between students, parents and educators should be purged regularly. Upon expiration of the retention period, proper method of disposal or destruction shall be instituted to ensure secure disposal of personal data.

3) E-Learning platform providers and manufacturers are called upon to:

a) **Be transparent about their data processing practices to both educational authorities and the individuals using the e-learning platforms.** Individuals should be provided a single point of contact to address privacy and data protection concerns related to each e-learning platform. They have a right to question a company's data management practices and to complain to a data protection authority if they are unsatisfied with the company's explanation or are concerned that personal data has been mishandled.

b) **Limit the purposes for collecting personal data as appropriate to context, and specify in their terms of services or other legal contracts when personal data may be disclosed.** Student data must never be repurposed or used for non-educational purposes without express consent, unless there is legislation allowing for the repurposing.

c) **Be clear, specific and consistent in their terms and conditions of services.** Companies should avoid using terms such as "educational purposes" that are overly broad and do not inform individuals in sufficient detail to understand how personal data is being used.

d) **Adopt Privacy Enhancing Technologies and apply the principles of Privacy by Design and by Default.** Practices and technologies that minimize or eliminate the collection and use of personal data should always be preferred, and their effectiveness should be routinely monitored and improved upon.

e) **Ensure that personal data is stored in compliance with local data protection legislation.** Administrative, physical and technical safeguards should be in place to ensure the lawful processing of all personal data in compliance with applicable requirements and avoid the risk of inadequate security.

4) Lastly, Members of the ICDPPC are called upon to:

a) Inform and raise awareness of the privacy risks and responsibilities of using e-learning platforms;

b) Use this Resolution to develop guidelines that assist educational authorities and e-learning platform providers and manufacturers in meeting their data protection and privacy obligations;

c) Promote this Resolution and its recommendations with stakeholders and policy-makers in their jurisdictions and networks;

d) Liaise with relevant international organizations and civil society groups to promote and follow up on the Resolution; and

e) Cooperate with each other and with the Digital Education Working Group to share resources, knowledge and best practices.

ANNEX TO THE RESOLUTION ON E-LEARNING PLATFORMS

This Annex contains TWO PARTS:

Part A. Complementary and Explanatory Notes; and,

Part B. Suggestions to Assist Members with the Implementation of this Resolution

Part A. Complementary and Explanatory Notes

The Resolution on E-Learning Platforms (the Resolution) builds upon previous work conducted by ICDPPC working groups and related networks, most notably the International Working Group on Data Protection in Telecommunication's Working Paper on E-Learning Platforms[1]; the Global Privacy Enforcement Network's 2017 GPEN Sweep Report on Online Educational Services[2]; and the Digital Education Working Group's Report on the Results of a survey on Educational Learning Platforms.[3] Taken together, there is a recognized desire for a resolution on e-learning platforms.

The Resolution addresses key privacy and security considerations relating to computer software, mobile applications, and web-based tools specifically provided to schools that students, parents and educators access via the Internet and use as part of an educational activity.

The recommendations are targeted mainly at educational authorities in their role as data controllers. These authorities can develop and enforce contracts and best practices for e-learning platform providers and manufacturers to ensure uses in accordance with the data protection laws and individual privacy rights. A number of recommendations are also directed at e-learning platform providers and manufacturers in their role as data processors, as they are in a position to develop their services in a data protection and privacy-sensitive way.

1 "Berlin Working Group Paper", https://www.datenschutz-berlin.de/pdf/publikationen/working-paper/2017/2017-IWGDPT_Working_Paper_E-Learning_Platforms-en.pdf.
2 "GPEN Sweep Report", https://www.ipc.on.ca/wp-content/uploads/2017/10/gpen-sweep-rpt.pdf.
3 "DEWG Report on Survey" https://icdppc.org/wp-content/uploads/2017/12/DEWG-Research-Paper-Canada-eplatforms_Sept-2017.pdf.

Definitions

For the purposes of the Resolution:

E-learning platforms refer to the online technological tools and media that assist in the communication of knowledge, its development and the interaction among educators, students and educational institutions. E-learning platforms typically involve a variety of devices (such as computers, tablets and mobile devices), data processing and usage models (in classroom, online courses) and actors (students, educators, educational institutions, platform providers, application providers).

The term excludes pure school management tasks operated on back office applications implemented by education authorities such as transfer and assignment of educators or administrative management of students at school that are not related to learning.

Personal data refers to the personal data of students, parents and educators. It includes identifiable information about them. This includes such information as a name, an identification number, location data, biographical, health and contact details, behaviour patterns, disciplinary records, special needs, and other information. It also refers to online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.

Educational authorities refer to those entities that establish curricula and set rules or frameworks on education. Educational authorities include ministries of education, their local representatives, school boards, schools, management staff, and educators.

Learning analytics refer to the measurement, collection, analysis and reporting of data about students and their learning practices, for the purposes of understanding and optimising learning

and the environment in which it occurs. Learning analytics includes “adaptive learning” practices, that is, the use of personal data to provide individualized teaching and support.

Recommendations

The following is offered to provide further context, explanation and examples related to the Resolution’s recommendations:

1) Educational authorities are called upon to:

a) Ensure they have authority and expertise to engage the services of e-learning platforms.

- Lack of legal authority and accountability introduces unnecessary data protection risks, and could result in privacy and security breaches, investigations and fines. Educational authorities may not have authority to collect, use or disclose some types of personal data, or to permit certain data processing operations by e-learning platforms. Educational staff, for their part, may lack authority to agree to third-party contractual terms on behalf of their school and students.
- Educational authorities should:
  - Take steps to confirm the applicable data protection and privacy laws and internal policy requirements that impact their authority to use e-learning platforms.
  - Ensure that responsibility for decisions to engage e-learning platforms are clearly assigned or delegated.
  - Consider whether there are any limitations on their authority to use an e-learning platform.

- Ensure that the agreement with the provider of e-learning platforms stipulates that the provider may only process student data in accordance with the instructions of the educational institution.[4]

- Use a written contract or legal agreement when possible, and take extra steps when accepting click-wrap licenses.[5] This includes, notably:

    - Ensuring the offer complies with local data protection laws and requirements;
    - Reviewing the Terms of Service to determine if the provider has retained the right to amend them without notice; and
    - Limiting authority on who can accept the Terms of Services or changes to it.[6]

- Where "click wrap" agreements do not meet data protection laws and internal policy requirements, educational authorities should not use those services.

b) Develop policies and procedures to evaluate, approve and support the use of e-learning platforms and, where feasible or required, conduct data protection/privacy impact assessments.

- To ensure compliance with applicable laws and internal policies, educational authorities need to take steps to understand how the e-learning platform processes personal data and identify the data protection and privacy risks that might arise, and the strategies to mitigate them. Lack of organizational readiness or understanding of the processing of personal data by e-learning platforms may lead to unexpected or unintended privacy and security risks such as breaches and inappropriate processing.

---

4 Berlin Working Group Paper, p. 6.

5 Click-wrap licenses or agreements are those in which a user must agree to terms and conditions prior to using the product or service.

6 For further information on this, see Privacy Technical Assistance Center, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*, ("EdTech Paper") pp 8-10: https://tech.ed.gov/wp-content/uploads/2014/09/Student-Privacy-and-Online-Educational-Services-February-2014.pdf

- Educational authorities should:
  - Develop methods to evaluate and mitigate privacy and compliance risks prior to implementing e-learning platforms.
  - Establish policies, procedures and operational standards for engaging e-learning platforms.
  - Promote and enforce compliance with school policies by students, parents, educators, and e-learning platform providers.
  - Facilitate individual control over personal data by enacting technical and organisational measures that support access, correction and other privacy rights in compliance with data protection law and policy.
  - Continuously monitor and improve technological and organizational measures for data security.
  - Conduct an inventory of the online educational services currently being used within your school or district to help assess the scope and range of student, parent and educator's data being shared with providers.[7]

EXAMPLE: Useful questions to pose when considering e-learning platforms include, but are not limited to: [8]

- Will any information about students, parents or educators be shared with parties outside the educational authority?
- Will you be sharing this information with companies or individuals that are not school employees? If so, who will have access?
- What types of information are being shared?
- Are there secondary purposes for the data that is being collected?

[7] EdTech Paper, p. 8. See also *The Common Sense Privacy Evaluation Initiative* for suggestions and example on conducting evaluation of e-learning platforms: https://www.commonsense.org/education/privacy.

[8] Berkman Klein Center for Internet & Society at Harvard University, Educational Technology and Student Privacy Checklist: https:/dlrp.berkman.harvard.edu/node/59.

- Will you obtain student or parental consent to share this information?
- What risks do you think sharing this information might pose to students? To you as an educator? To the school?

c) Provide training and on-going support for educators.

- If educators are not trained on the privacy implications of using e-learning platforms, then they may lack competence to select, deploy, configure and use e-learning platforms in a privacy-compliant way. For example, educators may not be well-equipped to guide students and parents on the appropriate use of these services.
- Educational authorities should:
  - Provide educators with a list of evaluated and approved e-learning platforms.
  - Provide educators with on-going information sessions about how the e-learning platform processes personal data and how to use it appropriately. This information should be adapted for use by parents and students.
  - Put in place equitable access to up-to-date equipment and resources, as well as appropriate, job-embedded, ongoing professional development to enable educators to learn about and experiment with new technologies.[9]
  - Raise awareness of data protection among students by inviting educators to incorporate the International Competency Framework for School Students on Data Protection and Privacy[10] into their teaching methods according to the age groups concerned.This may include, but is not limited to advice on how to:
    - Create an online account, user profile and online content;
    - Configure account settings and preferences;

[9] Media Smarts, *Connected to Learn: Teachers' Experiences with Networked Technologies in the Classroom*. p. 77: http://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/ycwwiii_connected_to_learn.pdf

[10] 38th ICDPPC, https://icdppc.org/wp-content/uploads/2015/02/International-Competency-Framework-for-school-students-on-data-protection-and-privacy.pdf

- Manage cookies, especially "third-party" tracking cookies;
- Download and install software, especially on personal computing devices; and
- Delete online content and/or accounts [11]

d) Work with other educational authorities and, in cooperation with local data protection authorities, to agree on common standards for engaging e-learning platforms.

- Failure to develop and apply common standards may result in the inconsistent application of individual privacy rights and obligations.
- Educational authorities should:
  - Facilitate cooperation and sharing of knowledge, best practices and other resources, including the use of pre-evaluated and approved e-learning platforms.
  - Develop and promote the use of model contract clauses, evaluation standards, certification marks, and Codes of Conduct.

e) Where required or appropriate, seek valid, informed and meaningful consent from individuals.

- Individuals must be able to exercise the data protection rights in relation to the processing of their personal data. This includes providing or withholding consent. When the use of the e-learning platform is compulsory, and without alternative options and opt-out mechanisms, the consent that is obtained is not valid, and may not be used as a legal basis for processing.
- Some circumstances may require express consent, such as when processing personal data that is sensitive in nature, for new, unexpected or inconsistent purposes, or when there is a risk of significant harm.

[11] GPEN Sweep Report, p. 8: https://www.ipc.on.ca/wp-content/uploads/2017/10/gpen-sweep-rpt.pdf.

- In the educational context where e-learning platforms are employed, there is an imbalance between students on the one hand and educational authorities on the other. The users of an e-learning platform may not feel free to abstain from the use of an e-learning platform when given the choice, since this may put them at a disadvantage compared to their peers. Under these circumstances, consent cannot be validly obtained.
- Certain data processing purposes may be prohibited. For example, some personal data collections, uses, or disclosures may have a discriminatory or harmful impact on individuals and would be inappropriate.
- Even where educational authorities have sufficient authority to engage and use e-learning platforms, individuals should have the right to opt out and receive educational services through alternative methods.
- Educational authorities should:
  - Be prepared to accommodate opt out choices.
  - Provide alternative means of instruction that do not require use of an e-learning platform.
- Where individual consent is the legal basis for data processing, educational authorities and e-learning platform providers and manufacturers should:
  - Ensure consent is provided directly by the individual in a way that is informed and specific.
  - Whenever necessary, obtain parental consent. When the targeted individuals include youth who are able to provide consent themselves, their maturity should be taken into account along with context.
  - Require express consent prior to disclosing personal information about students to a publicly-accessible site, where such practice is permitted.

f) Consistent with domestic law, implement a policy for individuals who access the e-learning platform with their personal electronic devices.

- Many educational authorities provide computers, tablets or other computing devices and the networked infrastructure for use by students, parents and educators. In other cases, students, parents and educators may use their own devices to connect with the school's networked infrastructure. There are additional data protection and privacy risks that arise when using a personal device.
- Educational authorities should mitigate those risks by:
  - Ensuring that their networked infrastructure is governed by clear and transparent usage policies.
  - Minimizing, and where appropriate prohibiting, the collection of individuals' personal data, from personal devices and personal data stored on the device that is unrelated to the educational service.

2) Educational authorities and e-learning platform providers and manufacturers are called upon to, jointly or independently according to domestic data protection law:

a) Make sure that e-learning platforms appropriately safeguard users' personal data and meet the appropriate data protection standards.

- Inadequate safeguarding of users' personal data creates unnecessary privacy and security risks, such as unauthorized use and disclosure of personal data. For example, sensitive student data could be exposed by the use of insecure login mechanisms, poor configuration of the platform, or human error, and require that additional security measures be in place.
- Legal agreements can ensure lawful processing by promoting effective control, accountability, and compliance. Contract provisions should support individual privacy rights and data protection obligations.
- Educational authorities and e-learning platform providers and manufacturers should:

- Ensure personal data protection requirements are part of any legal agreements regarding e-learning platforms, including "click-wrap" and negotiable terms of service agreements.
- Ensure legal agreements define types of personal data to be processed, the purposes for collection, uses and disclosures, the location of storage and processing, retention requirements, and access and correction rights. They should also set out the administrative, physical and technical safeguards and breach notification requirements.
- Allow for, and require, the use of a multi-factor authentication mechanism for administrators and educators to log in to the platform to prevent misuse through stolen passwords.
- Require access controls and logging policies to be in place and enforced to ensure that access to personal data is properly managed and supervised. Access to personal data should follow the 'need-to-know' principle.
- Encrypt data transmissions between servers and users of online learning platforms. Depending on the respective online learning platform, the use of the encryption technology has to be examined individually for this purpose.[12]
- Continuously monitor and improve the security controls.

- In the event of a breach, providers of e-learning platforms and educational authorities should notify educational institutions, students or their parents, and appropriate supervisory authorities in accordance with local data breach notification requirements.

b) Make sure that the purposes for which personal data are being collected, processed and used are legitimate, suited to the context and authorized by law.

- Limiting the use of student data for educational purposes, including in the context of student learning, is a protective measure of the rights of data subjects, especially minors;

[12] German National Conference of Data Protection Commissioners, *A Guidebook From the Data Protection Supervisory Authority for Online Learning Platforms in School Classrooms*, p. 22. English translation available at: https://www.datenschutz-berlin.de/pdf/orientierungshilfen/2018-OH_Lernplattformen.pdf

- These data are not to be used for commercial purposes, including for instance, the resale of data, and the reuse for direct or indirect dissemination of advertising.

c) Minimise the amount of personal data to be processed.

- Data minimisation principles should be applied at all times to reduce the risks of excessive or unauthorized collection, use, and disclosure of personal data.
- Educational authorities and e-learning platform providers and manufacturers should:
  - Evaluate whether personal data is required, and to what extent, to fulfill the education-related purpose.[13]
  - Provide options to opt-out of the data collection on e-learning platforms for students and parents who do not wish to provide their personal data.

d) Before collecting personal data, notify individuals about the personal data to be processed by the e-learning platform and the reasons for processing.

- Inadequate notice or lack of transparency have a negative impact on the principle of lawfulness and fairness, and hinders the individual's ability to make informed decisions and provide meaningful consent.
- Educational authorities and e-learning platform providers and manufacturers should:
  - Use privacy notices to proactively communicate, inform and engage individuals about how their personal data will be processed.
  - Present notifications in the most effective and appropriate manner suited for the context.

[13] See recommendations from section 3(b) and 3(c) of this document which sets out requirements to ensure the stated purposes are clear and suited to the educational context.

- Where possible, provide notices at registration through direct engagement with parents and students, informing them of their rights and how to exercise them.
- Where notices are directed at students, provide them with age-appropriate support to help understand the notices.
- Provide information about the types of information collected, the purposes for its use, and to whom the information may be disclosed.
- Include information about how aggregate and de-identified information will be used and disclosed.
- Notify individuals when a change to the data practices of the educational authority or e-learning platform provider has occurred.
- Provide contact information to the local data protection authority.

> **Example**: Most site privacy policies disclose the presence and use of third-party cookies but do not provide specific instructions or meaningful options for preventing or managing them. Third-party cookies can typically be blocked with no apparent loss of functionality. Many educators and students may not know how to block or manage cookies. E-Learning platform providers should provide meaningful options to block or manage cookies so individuals can navigate the platform without being tracked.[14]

e) As far as possible, allow individuals to use the e-learning platform with de-identified data.

[14] GPEN Sweep Report, p. 3.

- Excessive collection of personal data can expose a large amount of data to unnecessary risk of misuse and breach.
- Consistent with the data minimisation principle, and to the greatest degree possible, the identity of individuals and the identifiability of their personal data processed by the e-learning platform should be minimised or de-identified.
- Educational authorities and e-learning platform providers and manufacturers should:
  - Allow individuals to use the e-learning platform without registering for a personal account. Where a student identifier or account is needed, then pseudonyms should be created that do not reveal names or other personally identifiable data.
  - Where personal data must be collected by the e-learning platform, de-identify or aggregate the data at the earliest opportunity.
  - Avoid the use of social media login as it can result in excessive collection and disclosure of detailed profile and other identifiable information between the social networking site and the e-learning platform and can limit the students' ability to prevent the tracking of their online activities across the web.

> **Example:** E-Learning platform providers should advise educators to minimize personal information used to create a profile by assigning pseudonyms to students. Students could then access their profiles by inputting a unique access code provided to them. In this way, students do not need to provide their personal information and can use the service in a pseudonymous manner.[15]

f) As far as possible, avoid the use of personal data per se, and particularly data on learning behaviour, for predictive purposes, profiling or automated decision-making.

[15] GPEN Sweep Report, p. 3.

- While recognizing that personal data can be used as positive starting point to form educational decisions, the reliance on personal data for the sole purpose of predictive analysis raises serious concerns with regard to data protection, privacy and ethics.
- E-learning platforms which adapt the presentation of educational material to the individual learner collect data about and gauge students' capabilities and learning behaviour in order to increase the efficiency of the learning process. There is a risk in accumulating data about individual students to allow for this adaptation. It may nevertheless be seen as justified by the benefits achieved.
- Automatic assessments, and the creation of student profiles for use external to the educational activity at hand, however, has the potential to undermine the evolving capacities of children and youth.[16] Algorithms underlying automated assessments may incorporate biased assumptions while hiding them from scrutiny. By necessity, they need to operate on a limited set of data, and fail to take circumstances and challenges of individual students into account. Profiles based on observed learning behaviour threaten fundamental privacy and intellectual freedom rights.
- Where data is used for automated assessments or decisions which affect the students beyond the narrow confines of the educational experience provided by the platform, this process should be transparent to educators, students, and parents. The latter should always be provided the right to object to this use, and to challenge the resulting assessments and decisions.
- Educational authorities must:
  - Ensure that they retain full control over any determinations or evaluations made about students, especially in case of automated decision-making.
- Educational authorities and e-learning platform providers and manufacturers should:

[16] UNICEF, *Children's Online Privacy and Freedom of Expression*: https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

- Ensure transparency regarding the use of algorithms and profiles that may influence decision-making. Any associated automated decision-making or other rule-based systems and the reasoning underlying the determinations made with the systems must be explained to students and parents.
- In cases of automated individual decisions, provide access to the decision and its reasoning. There should be specific procedures that lead to a human evaluation of decisions in cases where a different point of view is submitted, counter-arguments presented, or where the decisions are challenged.[17]
- Make algorithms, protocols, designs and implementations open for external review and/or testing. Open audits, or audits by trusted entities, can help to provide assurance that the e-learning platform will not generate unfair or discriminatory outcomes.[18]
- Where data on learning behaviour is collected and used for predictive purposes and profiling, consider the recommendations in related ICDPPC resolutions including, specifically, the Resolution on Profiling adopted by the 35th ICDPPC.[19]

g) Embed and employ tools that enable individuals to control their personal data and effectively exercise their privacy rights, including their right to access, correction, erasure and, where applicable, data portability.

- Companies must design their e-learning platforms and services in a way that enables access, correction and erasure requests by students, parents, or educators, as appropriate. The failure to do so creates the risk that individuals are unable to exercise their privacy rights.
- Educational authorities should:
  - Avoid entering into agreements with e-learning platforms where the personal data of students is tied in a black-box processing platform with poor transparency and control.

[17] Berlin Working Group Paper, para 37.
[18] Berlin Working Group Paper, para 33.
[19] https://icdppc.org/wp-content/uploads/2015/02/Profiling-resolution2.pdf

- Where circumstances allow, facilitate the exercise of privacy rights by assisting the individual or acting on their behalf when dealing with e-learning platforms and remain accountable for ensuring that the rights are respected and protected.
- Educate students and inform parents of the tools that exist to exercise their privacy rights.

- Providers of e-learning platforms should:
  - Embed tools that enable the effective exercise of the right to access, correction and erasure.
  - Where data protection laws give individuals the right of data portability, ensure that the data is made available in a structured, machine readable and open format (e.g. to account for when a pupil changes school).

h) Set and respect retention periods for different categories of personal data.

- Retention policies or retention schedules list the types of record or personal data held, what it is used for, and how long it will be kept. They help establish and document standard retention periods for different categories of personal data, and support policies and procedures for secure destruction.
- Storing personal data longer than necessary for the purposes it was collected can expose personal data to unnecessary risk of misuse and breach. Students and parents have the right to access and correct educational records and any other personal data (including behavioural data) stored, regardless of who collects or maintains the data.
- Deleting personal data once it is no longer needed reduces the risk that it becomes irrelevant, excessive, inaccurate or out of date.[20]
- Educational authorities and e-learning platform providers and manufacturers should:

[20] For other reasons to adopt a retention policy, see UK Information Commissioner's Office, "Storage Limitation" https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/

- Publish information regarding the categories of data collected, the purposes for which the data will be used, the identity of the actors involved in the processing, how long the data will be kept, and the security practices in place.[21]
- Subject to other legal and regulatory requirements, ensure appropriate clarifications of the data processed by the e-learning platform.
- Minimize the retention of all personal data including data generated from the use of personal data, such as logs, assessments and profiles.
- Carry over data from one educational activity to another only under the full control of educators, and transparency to children and their parents. Data which is not carried over in this manner should be deleted after a reasonable retention period after the end of the activity.
- Delete individual accounts and the personal data associated with them after a predetermined period of inactivity and disuse, or upon request.

3) E-Learning platform providers and manufacturers are called upon to:

a) Be transparent about their data processing practices to both educational authorities and the individuals using the e-learning platforms.

- Students, parents and educators have the right to know what personal data is being collected about them and how it will be used, and to know when it may be disclosed to others. If the data processing practices of the e-learning platform are not fully transparent, there is the risk that educational authorities and individuals will be unable to make informed decisions about their participation in the platform.
- To ensure informed decision-making, e-learning platform providers and manufacturers should:

[21] Berlin Working Group Paper, para 30.

- Make readily available, and in understandable form, information about how they handle personal data.
- Clearly state the data processing practices to educational authorities prior to engaging in service agreements.
- Clearly state their data processing practices to students and parents upon registration for the service.
- Provide notice whenever modifying the terms of collection, use or disclosure of personal data. The notice should clearly articulate the change that is proposed, or has occurred.
- Provide educational authorities, parents and students with a point of contact able to answer questions about the platform's data processing practices.
- Guarantee the sustainability of their services through the duration of their agreement with the educational authority.

b) Limit the purposes for collecting personal data as appropriate to context, and specify in their terms of services or other legal contracts when personal data may be disclosed.

- The purposes for collection, use and disclosure must be suited to the educational context to avoid the risk of inappropriate, unauthorized or illegal data processing.
- E-learning platform providers and manufacturers should:
  - Process personal data solely in ways that are consistent with the educational context in which the data was provided.
  - Never reuse or share data related to students' use of the e-learning platform for incompatible or secondary purposes.
  - Never use personal data derived from the use of e-learning platforms for marketing and advertising purposes.

c) Be clear, specific and consistent in their terms and conditions of services.

- If the terms and conditions are not clearly and consistently made available, educational authorities are unable to make informed decisions when entering into agreements with e-learning platform providers.
- E-learning platform providers and manufacturers should:
  - Clearly define the purposes for which they are collecting personal data, and avoid vague terminology such as "educational purposes" and "educational quality" that permit overly broad collection.[22]
  - Apply the recommendations found within this document when developing clear and consistent terms and conditions of use, including provisions dealing with prohibited purposes, retention policies, and appropriate safeguards.

> **Example**: Specifying that a collection of data is necessary to "educational purposes" is overly broad. Specifying that the collection is necessary to "improve fifth grade reading skills" or "enhance college-level physics courses" more clearly articulates the reasoning behind the collection.

d) Adopt Privacy Enhancing Technologies and apply the principles of Privacy by Design and by Default.

- Privacy Enhancing Techniques ("PETs") help minimise the collection and use of personal data, improve transparency of data processing, and facilitate compliance with data protection

[22] For further examples of clear terms and conditions see: U.S. Department of Education's Privacy Technical Assistance Centre, *Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices*: https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Jan%202015_0%20%281%29.pdf.

rules. The use of PETs should result in making breaches of certain data protection rules more difficult and/or in helping detect them.[23]

- E-learning platform providers and manufacturers should:
  - Minimise the collection of personal data and use de-identified information consistent with Recommendations 2(b) and 2(e), and the principles of Privacy by Design and by Default principles.[24]
  - Take into account the protection of personal data both at rest and in transit.
  - Establish security controls to assure availability, integrity, confidentiality, durability and traceability of personal data that meet or exceed prevailing standards and practices.
  - Consider the Resolution on Privacy by Design adopted by the 32nd ICDPPC.[25]

e) Ensure that personal data is stored in compliance with local data protection legislation.

- In many cases, the personal data by e-learning platforms are not stored or processed in data systems under the control of educational authorities. Instead, many educational authorities rely on external, cloud-based providers to store and process student data. The use of cloud-based platforms may introduce new data processing risks related to transparency, security and accountability.[26]
- E-learning platform providers and manufacturers should:

[23] European Commission, *Privacy Enhancing Technologies (PETs) – the existing legal framework*, MEMO/07/159,May 2007: http://europa.eu/rapid/press-release_MEMO-07-159_en.pdf; Office of the Privacy Commissioner of Canada, *Privacy Enhancing Technologies – A Review of Tools and Techniques*, Nov. 2017, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/; European Union Agency for Network and Information Security (ENISA), *Privacy-Enhancing Technologies:* https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies; ENISA, *Privacy by Design*, https://www.enisa.europa.eu/topics/data-protection/privacy-by-design.

[24] See also Article 25 of the EU *General Data Protection Regulation*, "Data protection by design and default": http://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm

[25] https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

[26] Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April 2012, Sopot (Poland), pp. 1-3.

- Provide administrative, physical and technical safeguards to ensure the processing of all personal data is compliance with applicable data localization requirements.
- Allow regular audits carried out by data controllers, data protection authorities or other mandated auditing agencies, as the case may be.
- When using cloud-based services, ensure these meet or exceed prevailing data protection standards and practices for security, access and accountability.[27]
- Consider the resolutions that have been previously developed in these areas including the Resolution of Cloud Computing adopted by the 34th ICDPPC.[28]

[27] European Data Protection Supervisor, *Guidelines on the use of cloud computing services by the European institutions and bodies*; ENISA, "Cloud Security" page; NIST, *Guidelines on Security and Privacy in Public Cloud Computing*; ISACA, *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*.

[28] https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cloud-Computing.pdf

Part B. Suggestions to Assist Members with the Implementation of this Resolution

The Resolution and, in particular, its recommendations provide data protection authorities (DPAs) with a baseline from which they can work towards addressing the issue of e-learning platforms and their use of personal data. When implementing the Resolution domestically, DPAs are invited to consider the following actions:

a) Inform and raise awareness of the privacy risks and responsibilities of using e-learning platforms

- DPAs are invited to post the Resolution on their websites and other publications, share through communications and outreach channels, such as social media, and cite it in their work related to children and youth, and to education.
- As part of this effort, it is suggested that DPAs prepare educational resources (or leverage those prepared by others) and, where possible, act as a resource to offer information and share best practices. Efforts can include organizing informational sessions to raise awareness on the data protection risks and mitigation measures identified in this Resolution. These educational resources and informational sessions can serve to complement DPAs' efforts at empowering children and youth to know and to protect their privacy rights.

b) Use this Resolution to develop guidelines that assist educational authorities and e-learning platform providers and manufacturers in meeting their data protection and privacy obligations.

- DPAs are encouraged to use this Resolution as a starting point to develop guidelines related to e-learning platforms and their data processing practices.
- Guidelines can be specifically adapted to the local context and laws to help clarify the expectations and obligations incumbent upon the different actors in the e-learning environment. They should direct educational service providers towards delivering

adequate and high-level guarantees to accompany the collection, processing, retention and disclosure of students', parents' and educators' personal data.

- Guidelines also allow DPAs to look further into specific matters. For example, DPAs may want to look further into the use of learning analytics. Learning analytics may involve creating new and sensitive personal data used to create individual profiles and for analysis and prediction, and therefore should be subject to clear rules. The guidelines should define governing principles and serve as a strong ethical and privacy framework to govern the practices of learning analytics and to ensure compliance with data protection laws.
- Similarly, and where possible, DPAs should work with all stakeholders to develop Codes of Practice governing the use of e-learning platforms. Codes of Practice may be a good avenue for addressing matters related to the drafting of contracts of services by e-learning platform providers, setting minimum standards on what is to be found in said contracts.

c) Promote this Resolution and its recommendations with stakeholders and policy-makers in their jurisdictions and networks.

- DPAs can be instrumental in identifying, compiling and providing additional resources and knowledge. Moreover, DPAs may be in a favorable position to ensure policy-makers and other high-level decision-makers are aware of these resources as part of their deliberative process.

- DPAs are invited to share the Resolution with government and educational authorities and policy-makers, as well as to related industry sectors, parent groups and other relevant stakeholders in order to stimulate conversations on the important issues this Resolution addresses and influence related policies and laws.
- Raising awareness within the DPA's jurisdiction will help spread the Resolution's impact and facilitate the needed dialogue on e-learning platforms, appropriate data practices and, more generally, privacy rights in the classroom.

- For example, DPAs can partner with educational authorities in helping parents and educators better understand the personal data implications of using e-learning platforms. This knowledge may also help in contexts not covered by this Resolution (i.e. the use of online tutoring apps).

d) Liaise with relevant international organizations and civil society groups to promote and follow up on the Resolution.

- DPAs are encouraged to reach out to their contacts at international organizations and civil society groups that deal with data protection and privacy, with children and youth, with education and learning to share with them the content of this Resolution.
- These organizations and groups may provide additional perspective and expertise in further minimizing the risks and enhancing the benefits of privacy-friendly e-learning platforms. Further, they may help create regional and international leverage and coordination.

e) Cooperate with each other and with the Digital Education Working Group to share resources, knowledge and best practices.

- DPAs are urged to continue to work together and share their experiences in implementing this Resolution and, should enforcement actions arise, the results of their investigations.
- This sharing can be directly between DPAs, as well as through the different ICDPPC mechanisms, including notably to the Digital Education Working Group.
- For its part, the Digital Education Working Group is encouraged to continue researching and analysing the data processing practices of e-learning platforms, and to maintain a repository of Guidance and Codes of Practice developed by ICDPPC members or other stakeholders that relate to or refer to this Resolution.