Organisation for Economic Co-operation and Development

EDU/PISA/GB(2025)21/ANN1/REV1

For Official Use **English text only**

20 November 2025

DIRECTORATE FOR EDUCATION AND SKILLS
PROGRAMME FOR INTERNATIONAL STUDENT ASSESSMENT

Governing Board

FRAMEWORK FOR PERSONAL DATA PROTECTION IN PISA

This document sets out a revised version of the Framework for Personal Data Protection in PISA, which addresses comments received during the 60th meeting of the PISA Governing Board. In particular, Framework Requirements 6, 7, 11 (FR6, FR7, FR11) and paragraph 14, have been modified.

The PISA Governing Board is now invited to:

- **APPROVE** and **DECLASSIFY**, by written procedure by 11 December 2025, the "Framework for Personal Data Protection in PISA", set out in this document [EDU/PISA/GB(2025)21/ANN1/REV1].

Once approved, the Framework for Personal Data Protection in PISA will become the framework for personal data protection for the implementation of the PISA survey by countries and economies participating in PISA and the OECD, as joint controllers.

Background information as well as the rationale for the "Framework for Personal Data Protection in PISA" is provided in document [EDU/PISA/GB(2025)21/REV1].

Andreas Schleicher, Director for Education and Skills and Special Advisor on Education Policy to OECD's Secretary-General (andreas.schleicher@oecd.org)

JT03577157

Framework for Personal Data Protection in PISA

Introduction

Purpose of the document

1. The goal of the Programme for International Student Assessment (PISA) is to provide valuable insights into the knowledge and skills of 15-year-old students, by compiling data collected through tests and questionnaires into a database that supports comparative analyses. National and international reports, as well as secondary research based on these data, are used to inform policy at all relevant levels. Accordingly, processing of individual-level data and mutual sharing of Main Survey data in PISA serves important objectives of public interest by underpinning the production of high-quality reports and policy-relevant research. This document sets the framework for data protection that supports this goal.

2. This Framework for Personal Data Protection in PISA (also referred to as "the Framework") reflects a joint controllership arrangement between the OECD and the countries and economies participating in given PISA survey cycles (hereafter, "PISA participants").[1] It serves as a reference document for the OECD Secretariat, the PISA participants, the National Centres implementing PISA in their local context, and the OECD's contractors, collectively referred to in this document as "all parties". The Framework establishes mutual accountability for the protection of personal data, by defining a framework for personal data protection that all parties will follow throughout their implementation of a given PISA cycle. The Framework comprises 25 requirements, numbered from FR1 to FR25 and organised in five thematic sets: Digital security; Data protection information and individual rights for data subjects; Archiving of materials; Data transfers and data disclosure; Response to personal data breaches – data protection dispute. Each set is introduced by overall goals and rationale. This Framework is complemented and operationalised in instructions and manuals developed by the OECD over time.

3. A glossary of the personal data protection terms used in this document can be found in Annex A. Glossary terms appear in italics in the remainder of this document.

Stakeholders and roles

4. The OECD and the PISA participants jointly determine the purposes and means of *processing personal data* collected as part of the survey and therefore act as joint data *controllers*. Each PISA participant is a joint data *controller* specifically for the *processing* of *personal data* collected in their own country or economy.

5. The OECD, through its PISA Governing Board, is responsible for determining the standard survey and assessment design and the acceptable variations, for preparing the international version of survey instruments, and for reporting on its results at an international level.

[1] For the purposes of this document "PISA participants" refers to all countries and economies participating in a given PISA cycle (i.e. participating Members and non-Members, both "PGB associate members" and "PGB participants" as defined in the Resolution of the Council Renewing and Revising the Programme for International Student Assessment (PISA) [C(2021)88]).

6. PISA participants are responsible for managing the local implementation of PISA and ensure compliance with *applicable data protection regulation* in their respective jurisdiction, if necessary, by requesting agreed upon adaptations to the standard design. PISA participants may also analyse the resulting database and report on results in accordance with their own priorities.

7. The OECD may rely on contractors (and their sub-contractors) for all or part of the OECD's responsibilities. The OECD's contractors generally act as data *processors*. In this document, OECD's contractors are referred to as the "International Contractors". Any responsibility allocated to the International Contractors under this Framework shall be understood as the International Contractors acting on behalf of the OECD.

8. PISA participants may also rely on specialised agencies and contractors (local implementation partners) when managing the local implementation of PISA. In this document, local implementation partners are referred to as "National Centres" (NC); each National Centre is overseen by a "National Project Manager" (NPM). Depending on their relationship to the relevant national authorities, on their roles, and on the *applicable data protection regulation*, National Project Managers and National Centres may be considered either data *processors* or joint *controllers* of the *processing* of the data collected in their country/economy.

Scope

9. All parties will comply with the framework for *personal data* protection in PISA set out in this document. The Framework applies to the collection, transfer, disclosure and secure storage of survey data throughout the PISA cycles, including the processing of data for the purpose of analysis, reporting, or quality assurance. The Framework is designed to minimise risks for data subjects and to ensure alignment with the *OECD data protection rules* and with *applicable data protection regulations*, in particular with regard to secure data handling, mitigation of re-identification and *personal data breach* risks, and the protection of data subjects' rights. It does so by assigning specific responsibilities, as joint data *controllers*, to the OECD and to PISA participants.

Applicable data protection regulation – Legal basis for processing

10. Each party will comply with its obligations under the *applicable data protection regulation* and will ensure that it has a legal basis for *processing personal data* in its respective role.

11. The OECD will process any *personal data* in accordance with the *OECD data protection rules*. For the OECD, the legal basis for the *processing* of *personal data* in the context of PISA is the fulfilment of its mission, as well as the PISA mandate and approved programme of work.

12. PISA participants are responsible for determining the legal basis for PISA data collection and processing (e.g. legal mandates, public interest, consent) in their jurisdictions. Where the *applicable data protection regulation* requires the consent of data subjects for the *processing* of their data in PISA, National Centres are responsible for managing related procedures.

1. Digital security

1.1. Goals and rationale

13. All parties will ensure that all data is stored and processed in a secure and standardised manner in accordance with the Technical Standards approved by the PISA Governing Board. All parties will put in place robust safeguards against *personal data breaches*.

1.2. Data protection framework

FR1. The OECD and its International Contractors are responsible for selecting the software and applications that support sampling, case management, questionnaire-data collection, test administration and coding/marking operations by National Centres, as well as any software and applications used for transferring data between National Centres, International Contractors and the OECD. The selected software and applications integrate Privacy by Design[2] principles from the outset and all parties ensure that these Privacy by Design principles are maintained throughout the data lifecycle.

FR2. The OECD and its International Contractors are responsible for testing all above-mentioned software and applications prior to their release to National Centres. This process must ensure that the software is configured correctly to meet operational requirements, including the testing of any Privacy by Design elements built in the system, is free of technical issues and fully functional. Comprehensive testing must include performance, security and compatibility checks to guarantee a reliable user experience and to safeguard the integrity of data.

FR3. National Centres will use the above-mentioned software and applications as instructed by the OECD or its International Contractors and apply any updates or security patches within one week of receiving a new release. No other systems or tools will be used for the above-mentioned operations, unless otherwise agreed upon in writing.

FR4. A role-based access control model will be used by all parties to ensure that only relevant and authorised individuals can access these tools, and the data stored on them.

FR5. For any tools that rely on local installations, the computers hosting them will comply with the minimum requirements that will be set in the context of PISA Technical Standards.

FR6. The survey design will reflect the principle of data minimisation at every stage. In particular, any forms that contain direct identifiers, in digital or print format, such as sampling frames, login forms, tracking forms, etc., will be treated as highly sensitive information, kept secure at all times, with access strictly limited to authorised individuals only, and retained for a limited time (see below, "Archiving of materials"). The PISA participants and National Centres shall never share these forms or any information containing direct identifiers with the OECD or its contractors; nor shall any recipient otherwise be able, using any reasonably available means, to re-identify data subjects.

[2] Privacy by Design is an approach of systems engineering where any data protection measures are considered and implemented end-to-end in the engineering design process.

FR7. All parties ensure that their staff and *processors* involved in *personal data processing* activities are aware of and comply with the Framework for *personal data* protection in PISA. Each Party shall ensure the implementation of appropriate safeguards, including for collection, transfer, disclosure, and secure storage of survey data throughout the PISA cycles. The OECD will ensure that international contractors are bound by appropriate data protection clauses in this regard.

14. Data protection and digital security in PISA is supported by quality assurance procedures and quality records. Instructions and requirements for International Contractors are further detailed in contractual documents. Upon written request to the OECD Director for Education and Skills, the OECD will share with PISA participants a copy of the contractual clauses on personal data protection agreed with the International Contractors. Instructions and requirements for National Centres are further detailed in PISA Technical Standards and PISA manuals prepared and updated by the OECD and its International Contractors over the course of the project. PISA manuals are made available to National Centres through a central communication portal and document repository maintained by International Contractors.

2. Data protection information and individual rights for data subjects

2.1. Goals and rationale

15. All parties have a responsibility to respect and safeguard the autonomy, privacy, confidentiality and well-being of the data subjects, and to minimise the burden of study participation to the greatest extent possible, adhering to both ethical and legal obligations toward them.

2.2. Data protection framework

FR8. The OECD will prepare a model data protection notice and will make it publicly available. This model should be further adapted as necessary by PISA participants to meet local requirements. PISA participants and their National Centres are responsible for making data-protection information available to all data subjects. Data protection notices should clarify that the data released in response to an access request may not necessarily provide meaningful insight into a student's performance. The information provided to data subjects will include, at a minimum:

- contact details of the PISA participant and/or of its National Centre
- contact details of the OECD's Data Protection Officer and the OECD's Data Protection Commissioner
- the purpose of the *processing* of the data
- recipients or categories of recipients of the data, including the OECD, the International Contractors and any national contractors
- the storage location and retention period of data
- the existence of the rights of data subjects, including the timeline for facilitating these requests

FR9. Participation of students, parents, teachers and schools in PISA is voluntary unless otherwise stated by local legislation.

FR10. PISA participants will facilitate requests from data subjects to exercise their data rights. This may include, in particular, the rights to request access, rectification or erasure; to object to *processing* of their data; and to submit claims. PISA participants will also maintain a log of requests for access, rectification or erasure of data. If necessary, PISA participants and/or their National Centres will involve the OECD and its International Contractors in a timely manner to respond to these requests. In the event that the OECD directly receives a data subject request, the OECD will promptly forward the request to the relevant PISA participant and its National Centre. Requests for rectification or erasure may only be accepted for a period of four weeks following data collection, and before the submission of data to the international contractor in charge of weighting, as they could otherwise threaten the overall project goals and the statistical quality of the resulting database (i.e. its accuracy, coherence, accessibility, timeliness and reproducibility). All requests from data subjects should be acknowledged and either fulfilled or rejected within 30 days. That period may, where necessary, be extended by a further two months, taking into account the complexity of the request and the number of requests. In their handling of such requests, PISA participants and the OECD commit to the principles of transparency, fairness and accountability while safeguarding the privacy of other data subjects involved and the integrity of the project. Where requests cannot be fulfilled, PISA participants and/or the OECD provide a justification for their rejection. Where an extension of the 30-day limit is necessary to fulfil a request, the reasons for delay will be provided as well. In particular, where giving effect to requests for access, rectification and/or erasure would undermine the confidentiality of test materials, or create risks for other data subjects, requests may be legitimately rejected.

16. Instructions and requirements for National Centres related to this Framework are further detailed in PISA Technical Standards and PISA manuals prepared and updated by the OECD and its International Contractors over the course of the project. PISA manuals are made available to National Centres through a central communication portal and document repository maintained by International Contractors.

3. Archiving of materials

3.1. Goals and rationale

17. The OECD will maintain a central electronic archive of survey instruments and data for each PISA cycle for an indefinite duration. This will ensure continuity of PISA across cycles, and enable the OECD to build upon the knowledge gained in the course of a survey cycle for future projects of similar nature. PISA participants may also maintain an electronic archive of national survey instruments and data for similar purposes, or to pursue additional research opportunities.

3.2. Data protection framework

FR11. Central archiving by the OECD applies to both Field Trial and Main Survey instruments and data, and to any instruments used in preparatory work (e.g. pilot studies, focus groups, etc.). Central data archives will include only data transferred by National Centres or collected centrally for use in further *processing*. Central data archives are held on secure servers. Access to central data archives must be

authorised in writing by the OECD Director for Education and Skills. PISA participants can withdraw all data collected in their own country or economy from central data archives by submitting a written request to the OECD Director for Education and Skills.

FR12. National Centres will retain all Field Trial materials until the beginning of the Main Survey, and all Main Survey materials until the end of the calendar year two years after the year when the Main Survey is conducted or, at a minimum, until the publication of the first international report based on these data by the OECD. This includes also lists (sampling frames, tracking forms, etc.) that contain direct personal identifiers, which are never transferred to the OECD or its contractors. Should the *applicable data protection regulation* or other circumstances require that the Field Trial or Main Survey materials be deleted/erased earlier or later than this timeline, PISA participants and the OECD will agree upon a suitable variation of the timeline. Any costs resulting from a variation in this timeline will be borne by the PISA participant requesting it.

FR13. If data are archived by PISA participants to pursue additional research opportunities, e.g. to enable future linkages with external datasets, the *applicable data protection regulation* must be adhered to.

18. Instructions and requirements for archiving by National Centres are further detailed in PISA Technical Standards and PISA manuals prepared and updated by the OECD Secretariat and its International Contractors over the course of the project. PISA manuals are made available to National Centres through a central communication portal and document repository maintained by International Contractors.

4. Data transfers and data disclosure

4.1. Goals and rationale

19. PISA participants recognise the mutual sharing of Main Survey data with other PISA participants, and the transfer of Main Survey data to external researchers, as an important public interest objective of the Survey enabling comparative analyses and fostering policy-relevant research. All parties recognise that the quality of insights gained from statistical analyses is strengthened if the analyses behind published results are reproducible, meaning that the metadata, raw data, algorithms and software involved are clearly identified, openly accessible and properly documented. However, all parties also recognise that datasets that carry significant re-identification risks need to be protected from unauthorised access and use.

4.2. Data protection framework

FR14. All parties will ensure that any data published in national and international reports and in related interactive data querying interfaces (“data explorer”) are fully de-identified. The PISA Governing Board will set a “minimum group size” rule for statistical aggregates to ensure full de-identification.

FR15. The OECD is responsible for preparing the reference version of the de-identified databases for analysis and reporting, including through its International Contractors. All data preparation steps and methods used by the OECD and its contractors are fully documented and reproducible. The level of de-identification achieved in each database is documented in notes accompanying the database.

FR16. After the Main Survey, each PISA participant will receive its own national database (the "national database") for analysis and reporting, in an agreed-upon electronic format and according to a pre-specified timeline that may vary depending on data submission. This national database will contain the complete set of survey responses collected in that country/economy (in their original form or in a coded/scored version), with the sole exception of data erased at the request of data subjects.

FR17. Each PISA participant will also receive a second version of its own national database for inclusion in an international database collating data from all participants (the "international database", or IDB). This version will apply the same rules for data suppression, coarsening and data perturbation to all national databases, in order to reduce re-identification risks while preserving the database's value for comparative analysis and research.

FR18. PISA participants will need to sign a written arrangement with the OECD, which includes confidentiality and data protection provisions, before accessing the de-identified data of other PISA participants. The arrangement will explicitly list all authorised personnel and detail the permitted uses of these data. The OECD will not transfer or disclose the international database to signatories of the arrangements until all PISA participants, acting as joint *controllers*, have been given an opportunity to review and comment on the international database (in particular, to request additional de-identification measures), and have approved this transfer or disclosure to other PISA participants. Deadlines and procedures for this process will be decided by the OECD Secretariat and communicated to the PISA Governing Board.

FR19. The PISA Governing Board will decide on the inclusion, in the international database, of data for PISA participants whose data manifests significant technical anomalies that may negatively affect the statistical quality of the international database. The decision of the PISA Governing Board will be final. PISA participants may continue to use their own national data, even if excluded from the international database, at the national level.

FR20. The international database will form the basis of international reporting by the OECD.

FR21. After release by the OECD of the initial publication ("international report"), the OECD will make one or more versions of the international database publicly available on a cost-free basis. The OECD will conduct a data-disclosure-risk analysis on the international database and will propose the technical solution(s) for public access to these databases. The OECD Data Protection Officer will review the data-disclosure-risk analysis and the technical solution for public access to these databases. PISA participants will have an opportunity to request data suppression from this "public" version of the international database, taking into account the proposed solution, the results of the data-disclosure-risk analysis, and their national context and regulations. PISA participants accept that data that is not requested for suppression may be released by the OECD as part of the "public" version of the international database. Deadlines and procedures for this process will be decided by the OECD Secretariat and communicated to the PISA Governing Board.

FR22. PISA participants may decide on the modalities for accessing national databases by third parties and will bear all associated costs.

20. Instructions and requirements related to this Framework are further detailed in official PISA Governing Board documents and communications.

5. Response to personal data breaches – data protection dispute

5.1. Rationale

21. The accidental or deliberate exposure of *personal data* into a public or other uncontrolled or unauthorised environment can have serious consequences for data subjects, but also for data *controllers* and data *processors*. The faster a *personal data breach* can be detected and contained, the lower the costs for all parties involved.

5.2. Data protection framework

FR23. In case of a *personal data breach*, the party that first detects the incident must inform the joint data *controllers* (namely the OECD and the relevant PISA participant) as well as their respective Data Protection Officers. Notification will be made as soon as possible after its discovery and must include an incident report. The report must detail the nature of the breach, the affected data, and proposed mitigation measures. When the notification occurs more than 72 hours after the discovery, the reasons for delay will be provided as well. The OECD and the PISA participant will collaborate to identify the scope of the breach and to contain it, to identify the risks posed by the breach and address them, and to implement any further action, including notifying the affected data subjects if required by either the OECD Data Protection Commissioner or local Data Protection Authorities.

FR24. The OECD will maintain a log of all reported *personal data breaches* and implement corrective measures to prevent future incidents.

FR25. All parties are expected to have breach response plans in place to ensure preparedness and compliance.

Annex A. Personal Data Protection Terms and Definitions

a) applicable data protection regulation means: (1) in respect of the OECD, the OECD data protection rules; and (2) in respect of the PISA participant, any privacy and/or data protection laws and regulations in any relevant jurisdiction that apply to the processing of personal data by or on behalf of the PISA participant;

b) controller means a natural or legal person who, either alone or jointly with others, determines the purposes and means of the processing of personal data;

c) OECD data protection rules means the OECD internal rules on data protection, which are the only rules governing Personal Data protection that are applicable to the OECD. They are currently set out in the Decision of the Secretary-General on the protection of individuals with regard to the processing of their personal data, Annex XII of the Staff Regulations, Rules and Instructions applicable to Officials of the Organisation; (available at https://www.oecd.org/content/dam/oecd/en/about/data-protection/Decision-of-the-SG-on-Personal-Data-Protection.pdf)

d) personal data means any information relating to an identified or identifiable individual ("data subject");

e) personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, theft of, or access to, the personal data transmitted, stored or otherwise processed, and any other incident impacting the availability, integrity or confidentiality of the personal data;

f) processing means any operation which is performed on the personal data whether or not by automated means. The terms derived from this, such as "process" and "processed" shall be construed accordingly.

g) processor means a natural or legal person who processes personal data on behalf of a controller.