UNICEF Innocenti – Global Office
of Research and Foresight

unicef | for every child

CASE STUDY

Certification Schemes

Case study overview

Type of innovation in data governance: Certification schemes

Key innovator(s) in focus:

- US Children's Online Privacy Protection Act (COPPA) Safe Harbor Program
- Europrivacy and Interprivacy data protection schemes
- International Certification of Evidence of Impact in Education (ICEIE)
- UK Age-Appropriate Design Certification Scheme (AADCS)

Problem the innovation is trying to solve: Poor implementation of laws and regulations.

About the innovation in data governance: Certification schemes have been developed in several contexts related to children's data, including EdTech (educational technology), age assurance, and children's data protection more broadly. They aim to assess a company's performance against a set of regulations or voluntary standards.

Countries or regions of operation: United States, United Kingdom, Europe, Global

Time period: 2000–date

Problem the innovation in data governance is trying to solve

While many countries have implemented new laws and regulations to strengthen data governance for children, and the private sector has developed numerous standards, the effective implementation of these measures remains insufficient. Certification schemes are emerging as one of the tools to help address this problem.

They guide companies through detailed processes to meet published criteria, providing assurance to technology companies, the public and regulators that minimum standards have been met. Certification schemes do not replace voluntary or mandatory regulatory audits but are rather a complementary mechanism for companies to demonstrate compliance.

Certification schemes are typically developed and overseen by an independent certifying body that verifies whether companies or specific products are complying with relevant laws, regulations or standards.

United States: Children's Online Privacy Protection Act (COPPA) Safe Harbor Program

Origins and implementation

The Children's Online Privacy Protection Act (COPPA) Safe Harbor Program in the United States is the longest-standing certification scheme focused on children's data protection and privacy. The certification scheme enables industry groups and others to develop self-regulatory programme guidelines to facilitate the implementation of COPPA. These guidelines are submitted to the Federal Trade Commission (FTC) for approval, verifying they provide protections that are at least equivalent to, or exceed, those outlined in the COPPA Rule. Once approved, companies that comply with an FTC-approved Safe Harbor Program and adhere to its guidelines are deemed to be in compliance with COPPA.

> While many countries have implemented laws and regulations and the private sector has developed standards, effective implementation remains insufficient – certification schemes are emerging to help address this.

The Safe Harbor Program, established in 2000, includes six certifying organizations approved through the FTC. These organizations are required to demonstrate to the FTC that they effectively monitor the companies they certify, ensuring compliance with their self-regulatory standards. Safe Harbors must also take disciplinary action against companies that fail to adhere to these guidelines. This can include mandatory public reporting of actions taken by the industry group issuing the self-regulatory guidelines, providing consumer redress, making voluntary payments to the State or referring repeat violations to the FTC.

In 2022, US Members of Congress opened an inquiry into COPPA Safe Harbors, calling for stricter compliance and oversight standards. A particular concern was the need for greater transparency in the business relationships between the Safe Harbor and its members. Under the new COPPA Rule which was revised in 2025, Safe Harbors will now be required to publicly disclose their membership lists and report additional information to the FTC as part of efforts to increase accountability and transparency in the programmes.

Impact and benefits for children

The FTC stated in 2007 that the Safe Harbor certification scheme promotes industry self-regulation, which the FTC believes responds more swiftly and flexibly to the needs of consumers, businesses and a rapidly evolving marketplace compared to traditional statutory regulation. However, the degree to which the certification scheme has resulted in better practices related to children's data protection and privacy remains contested.

Evaluating the effectiveness of self-regulation is challenging without greater transparency and publicly available information about the certification process. Furthermore, the level of industry participation in the voluntary Safe Harbor Program is unclear, due to a lack of information regarding the percentage of child-directed products in the US marketplace that are certified under one of the six Safe Harbor schemes.

Europrivacy and Interprivacy certification schemes for data protection

The European Union (EU) General Data Protection Regulation (GDPR) includes over 70 references to certification and explicitly calls for the creation of a certification scheme that can serve as a common standard throughout Europe. Europrivacy was established as a voluntary certification scheme designed to assess, document and certify compliance of a company's or organization's data processing activities with GDPR requirements. It was recently further developed into an international and geographically neutral certification scheme, Interprivacy, aligned with Convention 108+ of the Council of Europe and several regional conventions and norms, such as the African Union Convention on Cybersecurity and the Protection of Personal Data.

Origins and implementation

Europrivacy was developed by academics through a European research programme, financed by the European Commission. It is managed by the European Centre for Certification and Privacy (ECCP) in Luxembourg and maintained by an international Board of Experts in data protection. The scheme is supported by a partner network that includes certification bodies, global and regional consulting and law firms, technology providers and other experts.

In developing the certification scheme, researchers analysed approximately 30 international treaties and regulations related to privacy and data protection, including key regional treaties such as the European Charter of Fundamental Rights. They then extended the baseline to incorporate GDPR principles and national obligations from both EU Member States and approximately 20 non-EU countries. Their goal was to develop a framework that helps stakeholders navigate the complexities of complying with privacy and data protection laws across different jurisdictions. Interprivacy provides a more geographically neutral version of the certification scheme and can be used in any jurisdiction.

The ECCP itself does not provide certification or consulting services; instead, it focuses on maintaining the scheme and fostering the Europrivacy ecosystem. For the ECCP, the most important aspect of Europrivacy is to guide businesses and organizations through this process, helping them achieve compliance. This is especially critical for small and medium-sized enterprises that may lack dedicated compliance teams or may not fully recognize the need to address children's privacy in their compliance processes.

Impact and benefits for children

Improved compliance by tech companies with European and global data protection and privacy standards can significantly improve the landscape of data governance for children. Although Europrivacy does not currently offer a bespoke certification scheme focused on children's data, it is a general GDPR certification that could be used, for example by EdTech companies, as a basis for compliance. That is because data protection standards apply equally to children and adults, with some offering additional, tailored protections for children's data.

The Europrivacy scheme will soon undergo an impact assessment, as it has been officially recognized by the European Data Protection Board and will subsequently be subjected to regular monitoring and assessment. Given the scheme's progressive nature, there are potential opportunities to expand its scope and focus to include certification schemes covering specific areas such as data governance for children, or data governance for children in health, education or other domains. By aligning its requirements with international treaties, such as the Convention on the Rights of the Child, and emerging children's privacy frameworks, including the forthcoming EU Code of Conduct on Age-Appropriate Design, the scheme could become more child-centred in its approach.

Global: International Certification of Evidence of Impact in Education (ICEIE)

In addition to general data protection and privacy certification schemes, sector-specific certifications are also emerging, including for the EdTech sector. Researchers have identified 500,000 educational apps available on the Google Play and Apple App stores, making it challenging for educators and institutions to select and procure high-quality EdTech tools that also include strong data and privacy protections. The International Certification of Evidence of Impact in Education (ICEIE) certification scheme seeks to assist schools, teachers and parents in choosing EdTech tools that adhere to best practices in data governance and algorithmic fairness.

Origins and implementation

Launched in 2024, the ICEIE certification scheme emerged from an international research endeavour aimed at aligning diverse ways in which evidence and impact are documented in education. Using the 5 Es framework (Efficacy, Effectiveness, Ethics, Equity and Environment), the ICEIE certification aims to guide schools, decision makers and parents in selecting high-quality EdTech. The scheme offers three certification levels—Gold, Silver and Bronze—based on benchmarks of educational efficacy and effectiveness, with additional criteria related to ethics, including data protection and privacy. Similar to the ECCP's role in the Europrivacy scheme, the ICEIE does not deliver certification or consulting services itself, but rather focuses on creating the certification criteria and advancing a more harmonized global EdTech certification ecosystem under one umbrella.

The ICEIE Ethics criteria require EdTech products to provide evidence of compliance with data governance and data protection standards. The criteria cover four key domains: data governance and fairness, accessibility and interoperability, privacy and inclusivity, and algorithmic fairness (for EdTech tools based on artificial intelligence). For the domain on data governance, the product may have already complied with Institute of Electrical and Electronics Engineers (IEEE) standards or possess an iKeepSafe Certification (one of the US COPPA Safe Harbor seals). If not, a list of guiding questions assists reviewers in evaluating the product. To achieve certification, EdTech companies are recommended to collaborate with one of the ICEIE's affiliated certifying bodies to demonstrate their adherence to the criteria outlined in the certification scheme.

The ICEIE certification is valid for two years, after which the EdTech organization can apply for recertification. The certificates are publicly available documents.

Impact and benefits for children

Given that the certification ecosystem for data protection, privacy and artificial intelligence (AI) ethics is still evolving, there are few certifying bodies capable of validating EdTech companies seeking the Ethics certification. However, since data protection, privacy and AI ethics are critical concerns in the EdTech sector, widespread adoption of the ICEIE Ethics certification could significantly raise data governance standards for children.

United Kingdom: Age-Appropriate Design Certification Scheme

The Age-Appropriate Design Certification Scheme (AADCS) is based on the United Kingdom's Children's code, which was developed and published by the Information Commissioner's Office (ICO) in 2021.

Origins and implementation

The UK ICO is the first regulator to approve a certification scheme based on a Children's code. By enabling certification in children's data protection, the ICO has established a binding framework that organizations and companies can join.

The aim is to raise data protection standards and ensure that companies consistently adhere to the latest best practices in a constantly evolving regulatory landscape. This also provides companies with a clear opportunity to demonstrate their commitment to their clients, suppliers and the public.

The UK ICO is the first regulator to approve a certification scheme based on a Children's code.

The certification scheme is owned by the company Age Check Certification Scheme Ltd. (ACCS), which has a service-level agreement with Avid Certification Services Ltd., a UKAS-accredited conformity assessment body. The ICO-approved certification criteria are based on the provisions of the Children's code. Currently, ACCS is the sole certification body for the Children's code scheme approved by the ICO.

Impact and benefits for children

As of February 2023, five organizations had received certification under this scheme, with others still navigating the process. Given the size of the tech company ecosystem in the UK, this remains a relatively small number. As a result, the impact on children's data governance is likely to be limited unless a larger number of companies pursue certification, which could help raise standards across the entire sector.

Lessons learned

Some of the common experiences and lessons learned under these certification schemes include:

Cost of developing and maintaining a certification ecosystem: When a certification body is administered by a private company (such as the US Safe Harbors or the UK AADCS), it must be commercially viable, which means that the investment required to set up the scheme must be justified by the number of companies seeking certification that are willing to pay the necessary fees. For publicly funded or grant-supported academic projects, such as Europrivacy, Interprivacy and the ICEIE, maintaining and updating certification schemes can be challenging without long-term resourcing, which is often difficult to secure outside the private sector.

Incentivization for tech companies: For tech companies, particularly start-ups, developing and maintaining compliance with certification standards can be costly. To encourage participation, it is essential to provide clear benefits that outweigh these costs. Ensuring that certification schemes are affordable for small and large tech companies alike is challenging. Where procurement rules mandate certification as a prerequisite for public contracts, it provides an additional incentive for companies to engage with certification schemes.

Transparency and accountability: Publicly funded certification schemes generally result in certification criteria which are transparent and published as a public good. In contrast, private certification bodies often consider the details of their certification process proprietary and may not disclose the names of their clients.

By making evaluation criteria, certification results and the names of the evaluating bodies or validators publicly available, the process promotes accountability among companies and enables consumers to make informed decisions, knowing that certified products have undergone thorough, independent assessments.

Importance of regulatory or government oversight: Certification processes are typically conducted by certification bodies, which are often private companies themselves. To fulfil their duties under the UN Guiding Principles on Business and Human Rights (UNGPs), States must ensure that they provide effective oversight over the certifying body itself—for example, by carrying out periodic audits. Furthermore, ISO standard 17065:2012 requires certification schemes to be accredited by a national accreditation body, to help ensure consistency and integrity in the process.

Global applicability and replicability: Tech companies may face challenges certifying their products for use across multiple markets, especially concerning children's data governance. However, both Interprivacy and the ICEIE have worked to incorporate a more internationally representative set of criteria into their certification schemes. Notably, there does not appear to be any certification scheme relating to children's data protection and privacy operating in the Global South, highlighting an area for future development.

Conclusion

When properly designed, certification schemes provide regulators with a valuable tool to enhance oversight and compliance across the diverse technology subsectors, serving as an efficient compliance mechanism to demonstrate the implementation of laws and policies related to children's data. Nevertheless, regulators must retain ultimate responsibility by ensuring robust oversight over both certification bodies and the schemes themselves.

By undergoing a certification process, companies are scrutinized for their capacity to safeguard children's data, as well as their commitment to upholding children's privacy, safety and overall well-being.

About this case study

This case study is part of the UNICEF Innocenti – Global Office of Research and Foresight Data Governance for Children project, which aims to work with policymakers, industry, civil society and children to inform better data governance for children. This case study was written by Emma Day and Veronique Lerch, under the guidance of Jasmina Byrne and review by Melanie Penagos. We are grateful to the following individuals for their invaluable contributions and comments: Natalia Kucirkova, ICEIE; Jim Siegl, Future of Privacy Forum; Tony Allen, ACCS; and Maximilian Bleyleben, founder and investor. This project is made possible by funding and support from the Ministry for Foreign Affairs of Finland. We are grateful for their continued partnership and commitment to child rights.

In 2021, UNICEF published the Manifesto on Good Data Governance for Children, which contains recommendations and principles for governments and industry to create laws, policies and practices regarding child-centred data. One of the Manifesto's key recommendations was for stakeholders to initiate more policy innovations in data governance for children. This case study forms part of a collection of case studies detailing examples of such policy innovations for children in a diverse range of contexts. The approaches taken, lessons learned and insights gathered will be one contribution to the global effort towards better data governance for children. View all the case studies on the UNICEF website.

About us

UNICEF works in the world's toughest places to reach the most disadvantaged children and adolescents and to protect the rights of every child, everywhere. Across 190 countries and territories, we do whatever it takes to help children survive, thrive and fulfil their potential, from early childhood through adolescence.

And we never give up.

UNICEF Innocenti – Global Office of Research and Foresight tackles the current and emerging questions of greatest importance for children. It drives change through research and foresight on a wide range of child rights issues, sparking global discourse and actively engaging young people in its work.

UNICEF Innocenti equips thought leaders and decision-makers with the evidence they need to build a better, safer world for children. The office undertakes research on unresolved and emerging issues, using primary and secondary data that represent the voices of children and families themselves. It uses foresight to set the agenda for children, including horizon scanning, trends analysis and scenario development.

The office produces a diverse and dynamic library of high-level reports, analyses and policy papers, and provides a platform for debate and advocacy on a wide range of child rights issues.

UNICEF Innocenti provides, for every child, answers to their most pressing concerns.

Cover photo:
© UNICEF/UN0668616/Dejongh

Published by

UNICEF Innocenti – Global Office of Research and Foresight

Via degli Alfani, 58

50121, Florence, Italy

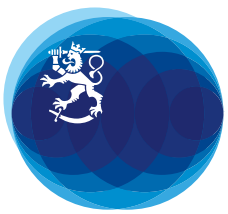
Tel: (+39) 055 20 330

Email: innocenti@unicef.org

Social media: @UNICEFInnocenti on Facebook, Instagram, LinkedIn and YouTube

Generously funded by

Ministry for Foreign Affairs of Finland



Ministry for Foreign Affairs of Finland

unicef

for every child