

**SIIA**Accelerating Innovation in
Technology, Data & Media202.289.7442
www.siia.net1090 Vermont Ave NW Sixth Floor
Washington DC 20005-4905

5 April 2019

Children's Consultation
Data Protection Commission
21 Fitzwilliam Square
Dublin 2

To Whom It May Concern:

I am writing to you on behalf of the Software & Information Industry Association (SIIA), which is the principal trade association for the software and digital content industries worldwide. The association provides global services in government relations, business development, corporate education, and intellectual property protection to its members, the leading companies that are setting the pace for the digital age. SIIA is engaged in the European policy debate and has organized conferences and events on issues of interest to European policymakers in Brussels, London, Berlin and Geneva, as well as in Washington, D.C. SIIA has submitted comments to the Article 29 Working Party on data breach, automated decision making, and data portability. SIIA submitted this letter to the British ICO in response to the "Consultation: Children and the GDPR Guidance." SIIA has member companies that market directly to children. SIIA is also a very active participant specifically in education technology policy discussions, including with respect to student privacy. We are registered in the European Commission's Transparency Register (ID number: 502425118410-86.)

We write to comment on three questions outlined in the public consultation document:

1. Data protection by design and default question 15;
2. Online service providers and different national ages of digital consent in the EU question 11;
3. Children and the GDPR in Education.

Data protection by design and by default

Organisations whose products or services are offered to children are aware of the special considerations that must be in place to protect children. Laws around the globe enacted over the past several decades have set policymakers' expectations of how organisations should protect a child's privacy. Older children will likely be savvier about the internet and, while Ireland has set a higher age of consent, special considerations should be made for evolving capacities of a child.

SIIA encourages the Irish DPC to work with its European Data Protection Authority counterparts to identify best practices on this topic.

Compliance with differing laws across borders

One of the primary reasons for developing the GDPR was the idea – strongly supported by SIIA – that it would be beneficial both for consumers and children, as well as industry, to have uniform EU-wide data protection rules. Therefore, SIIA strongly urges the EU to have a common age of consent, preferably 13. To the extent there are divergences in Member State law, industry will of course comply. In the digital age, however, this may imply the use of geoblocking or geofencing tools. It is all too easy to imagine a 15-year-old from Member State A with an age of consent of 16 accessing content or services from Member State B with an age of consent of 13 if there are no tools available to prevent this from happening. SIIA wrote about this in a White Paper entitled: “Geolocation Tools and Geographical Market Segmentation.”¹ SIIA notes in that paper that: “Websites and online content providers often use technical means to ascertain the geographical location of potential visitors. They do this for a variety of socially beneficial purposes, including localizing content, fighting online fraud and complying with local laws and regulations. Proposed bans on these geolocation techniques would halt these uses.”² Going forward, it will therefore be important for the EU not to interpret the Geo-Blocking Regulation in a way that would prevent companies from using geolocation tools to comply with differing Member State laws.

Children and the GDPR in Education: Guidance for Educational Institutions

The majority of SIIA member companies in the education sector provide services pursuant to contracts with education authorities. As a result, they are typically data processors, not data controllers. This does not mean of course that data processors do not have responsibilities. They do per the GDPR’s Article 28. The question of how personally identifiable information, including of children, is to be used must be in compliance with GDPR and be determined in a contract between the data controller and the data processor according to Article 28. This is consistent with current practices in the marketplace. SIIA therefore considers that it would be helpful for the Irish Data Protection Commission (DPC) and Data Protection Authorities throughout Europe to remind education technology marketplace participants to review their contracts to ensure that they are consistent with the GDPR’s requirements.

¹ SIIA White Paper, “Geolocation Tools and Geographical Market Segmentation,” 2014
https://www.ftc.gov/system/files/documents/public_comments/2014/04/00010-89273.pdf

² SIIA White Paper, Page 2

Moreover, SIIA recognizes that in a changing education technology landscape, it has become increasingly important to identify best practices to protect student information and data sharing as more education stakeholders want access to student data. Those practices can include:

- 1) Collecting, sharing, and using student PII only for education-related purposes;
- 2) Providing transparency regarding the type of PII being collected in privacy notices;
- 3) Appropriately vetting third parties collecting PII;
- 4) Ensuring security to protect student information against risks of unauthorized access or use;
- 5) Confirming data retention, student rights, and how schools should respond to user requests for access to data.

SIIA would be pleased upon request to share additional perspectives on the protection of a child's data under GDPR. Please contact me at [REDACTED] with any additional questions.

Thank you,

[REDACTED]
[REDACTED]

Software & Information Industry Association