LAW LIBRARY
LIBRARY OF CONGRESS

Children's Online Privacy and Data Protection in Selected European Countries

European Union
Denmark • France • Germany • Greece • Portugal
Romania • Spain • Sweden • United Kingdom

April 2021

Report for Congress
LL File No. 2021-020137

The Law Library of Congress, Global Legal Research Directorate
(202) 707-5080 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

Contents

Comparative Summary

Clare Feikert-Ahalt
Senior Foreign Law Specialist

I. Introduction

This report surveys how selected countries from the European Union (EU), namely **France, Denmark, Germany, Greece, Portugal, Romania, Spain, Sweden, the United Kingdom** (UK) and the laws of the **European Union (EU)** itself, provide privacy rights for children online.

The **EU** introduced the General Data Protection Regulation (GDPR) in 2016. As a regulation, the GDPR is directly applicable in all Member States, but most Member States have introduced legislation to ensure consistency and compliance with the GDPR in their domestic laws. The GDPR also contains clauses that permit derogation in certain areas to allow Member States to incorporate elements of the GDPR into their national law "as far as necessary for coherence and making it comprehensible." While the **UK** is no longer a Member State of the **EU**, it incorporated all **EU** law as it stood on December 31, 2020, into a new body of domestic law known as "retained EU legislation."

The **EU's** GDPR regulates the processing of personal data and establishes several principles that those processing personal data must comply with: lawfulness, fairness, transparency; limitation of purpose; data minimization; accuracy and keeping data up to date; storage limitation; and integrity and confidentiality. Article 6 provides the circumstances under which data processing is lawful; the most common circumstance is where consent has been provided by the data subject.

France, Denmark Germany, Greece, Portugal, Romania, Spain, Sweden, and the **UK** have introduced legislation that serves to implement or codify the GDPR in the country's domestic legislation. **Germany** amended its Federal Data Protection Act to incorporate elements of the GDPR into its national law. **Denmark** introduced a new Data Protection Act. **Spain** enacted the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (LPDP), which aims to protect the privacy and integrity of the individual and comply with the Spanish Constitution. The **UK** incorporated the GDPR into its national law through the Data Protection Act 2018. **Portugal** enacted Law No. 58 of 2019, which applies to the processing of personal data carried out within its territory. **Greece** enacted Law No. 4626/2019 to implement the GDPR. **Romania** amended over 1,500 of its laws and regulations to ensure its domestic laws complied with the GDPR. **Sweden** codified the GDPR in Swedish law through the Law on Additional Provisions to the EU Data Protection Regulation. **France's** Civil Code provides for a right to privacy, and it has also adopted the Loi Informatique et Libertés (Law on Information Technology and Freedoms), which states information technology "should not infringe upon human identity, human rights, privacy, or public or individual freedoms."

Denmark, Greece, Germany, Spain, and **Sweden** have constitutional provisions that provide additional protections to data collection and processing to protect an individual's right to privacy. **Denmark's** Constitution protects the right to privacy. **Greece's** Constitution protects against the unauthorized collection, processing, and use of personal data, and enshrines a persons' right to

participate in the information society as well as the right to protect against unauthorized collection, processing and use of personal data. **Germany's** Constitution provides individuals with the right to decide which personal data they would like to disclose and how such data will be used through the basic rights to confidentiality and integrity of information technology systems and informational self-determination. **Spain's** Constitution provides that the use of information technology must guarantee the personal and family privacy of citizens. **Sweden's** Constitution protects against the unlawful compilation of personal data.

II. Data Protection for Children

The **EU's** GDPR provides that consent from a parent or legal guardian must be provided to enable companies to process personal data for children under 16 years of age, and this age is used in **Germany** and **Romania**. The GDPR allows countries to provide lower ages of consent. **France** and **Greece** require the consent of a legal guardian for children under 15 years of age; **Spain** considers minors to be under 14 years of age; and **Denmark, Portugal, Sweden** and the **UK** set this age for consent at 13 years of age. The **EU's** GDPR requires that information provided to children about the processing of their personal data must be presented in clear and simple terms that are easily understood.

In the **UK**, the data controller has a duty to verify that the individual providing consent for the child has parental responsibility for the child. **Portugal** requires permission from a legal guardian to be obtained through a secure means of authentication. **Germany** and **Romania** require data controllers to make reasonable efforts to verify that the person with parental authority has given consent on behalf of the child; however, both countries do not specify and have not issued any guidance over how the age of children should be ascertained. A recent court decision from **Germany** has noted that a barrier requiring the input of a passport or ID number or credit card number with a minimal amount withdrawn from the account is insufficient and recommended instead the use of other, more technical measures, such as biometric information.

Other than requiring the consent of a legal guardian to process data for children, **France**, **Greece**, and **Spain** do not distinguish between children and adults for data protection rights, which are contained in the **EU's** GDPR and include the right to be forgotten, right of access, right to rectification, right to limit treatment, right of portability, and the right to object to the use of personal data for marketing purposes. **Spain** places a duty on legal guardians to ensure that children use digital devices and online information in a manner that "guarantee[s] the adequate development of the [child's] personality and preserve[s] their dignity and fundamental rights."

The **UK** is the only country surveyed to have issued a code specifically designed to protect children online. The **UK's** code, titled *Age Appropriate Design: A Code of Practice for Online Services,* was introduced in September 2020 and has a 12 month transition period, entering into force in September 2021. The Code aims to put children's interests first and protect them from within the digital world. It is comprised of 15 design standards, firmly placing responsibility on information society services to "take responsibility for ensuring that the way their services use personal data is appropriate to the child's age, takes account of their best interests, and respects their rights." The Code will be overseen by the **UK's** Information Commissioner, which has the power to take action, including issuing fines, to ensure compliance. The Code is not new law and sets out 15 cumulative, interlinked standards of design, detailing how the principles, rights and obligations

provided for in the **UK's** Data Protection Act apply to children, defined as anyone under 18 years of age. It is anticipated that most internet society services that are likely to be accessed by children will have to be redesigned to comply with the Code.

In **Sweden**, government agencies have issued combined guidance for children's rights online. The guidance provides that nudging techniques should not be used except to increase protection for personal data, and that age verification measures should be in place to ensure that a child does not misrepresent their age.

Denmark's Data Protection Authority has not issued guidance specifically relating to children and data protection, but has instead included them under guidance detailing how personal data collected from vulnerable groups should be handled. According to this guidance, an impact assessment must be conducted over how data collected from these groups should be processed.

In **Spain,** the Law on Services of the Society of Information and Electronic Commerce provides that public administrations must promote voluntary codes of conduct that take into account the protection of minors. No such code has yet been published. **Portugal** has also not introduced any code on the standards of age appropriate design that applies specifically to children.

With respect to enforcement, the **EU's** GDPR provides countries with the ability to issue fines of up to 4% of a company's worldwide revenue for violations of the provisions of the GDPR. **Sweden** has capped fines for certain violations at US$600,000 and US$1.2 million. Depending upon the severity of the infraction, infringements of **Spain's** data protection laws can be enforced through a series of monetary penalties, warnings, and disciplinary sanctions. The national regulator in **Romania** has the ability to apply both sanctions and corrective measures to both public authorities and private data operators that violate the provisions of the GDPR, including fines for each day that the data controller fails to comply with measures required from the regulator. In Denmark, the regulator considers violations involving the consent of children to be among the most serious infringements and this is taken into account when determining any fines, which in accordance with the **EU's** GDPR are required to be "effective, proportionate and dissuasive."

In **France,** mishandling personal data in or through a computerized system is punishable under the French Penal Code. Infringing the rules of the GDPR or the Loi Informatique et Libertés can result in substantial fines and up to five years in prison.

III. Advertisements on Platforms Designed for Children

The **EU, Denmark**, **Germany**, **Greece**, **Portugal**, **Spain, Sweden, Romania,** and the **UK** have laws that prohibit advertisements to minors on certain age-restricted products, such as alcohol, tobacco, e-cigarettes, and gambling. The age range of minors varies according to the type of product, but the restrictions typically apply to those under 16 or 18 years of age. In the **UK**, a code that applies to online advertisements provides that no age-restricted advertisements should appear in media directed to a protected age category and that measures should be used in directed advertisements to ensure children in the protected age categories do not receive them. **Spain's** laws include prohibitions on advertising on vending machines and information society services to children. **Germany**, **Greece, Portugal**, and the **UK** prohibit the advertisements for food

and beverages with high fat, salt or sugar content to be aimed at children aged under 16 years. **Greek** law encourages video-sharing service providers to adopt industry codes of conduct or take other measures to prevent minors from excessive consumption of food and beverages that are not appropriate for them.

Denmark has special rules that apply to advertisements directly targeting children, prohibiting the promotion of violence, and requiring them to be designed with "special consideration to the child or youth's natural credulity and lack of experience and critical sense." **Germany, Greece, Portugal,** and the **UK** have similar laws, requiring advertisements directed at children to take into account a child's psychological vulnerability.

The **EU's** Audiovisual Media Services Directive (AVMSD) aims to protect children, and has been extended to cover video sharing platforms and audiovisual content shown on social media sites. Video sharing platforms are under an obligation to take measures, such as age-verification or parental control systems, to protect minors from advertisements that may impair their physical, mental, or moral development. The **EU's** AVMSD prohibits audiovisual advertisements from directing minors to purchase goods or services; from encouraging minors to persuade their parents to purchase goods or services; from including elements that endanger a minor's physical or moral integrity or health and safety; or from exploiting the special trust that minors have in their parents, guardians or teachers. **Greece** and **Spain** prohibit advertisers on video sharing platforms from such advertisements. **Germany**, **Portugal, Romania,** and the **UK** apply these prohibitions to any form of advertising. **Romania** and the **UK** further provide advertisements featuring children should not encourage dangerous or irresponsible practices or utilize unsuitable, offensive, or distressing material.

Greece requires video sharing platforms to take appropriate measures to ensure that children are protected from "programs, user-generated videos and audiovisual commercial communications which may impair their physical, mental or moral development" and requires the most harmful content, such as gratuitous violence and pornography, be subject to strict access control measures. Any personal information collected through age-verification processes or parental control measures may not be used for commercial purposes, such as marketing or behavioral advertising.

In **Sweden** and **Denmark**, advertising rules are based on good practice and custom. In **Sweden**, advertisements targeting children are, in practice, prohibited. This applies to advertisements placed online, including those that are part of a game. **Sweden, Denmark,** and the **UK** require online advertisements, including those on blogs and social media, to be clearly marked to indicate they are advertisements. In **Sweden**, these types of advertisements may never target children.

France does not appear to currently have any specific laws or regulations that govern online advertising targeted at children.

In **Greece**, **Sweden**, **Romania,** and the **UK**, advertisements are self-regulated and compliance is enforced by domestic bodies. In **Denmark**, the Consumer Ombudsman is responsible for enforcing these laws.

IV. Future Plans to Protect Children Online

The **EU** is currently in the process of replacing its ePrivacy Directive with an ePrivacy Regulation. Depending on any new provisions this Regulation has, it may have implications for the protection of children online. The **EU** Strategy also states that in 2021, the European Commission will propose "legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities." The **EU** has also published a call for proposals for a pilot project to work on the technical infrastructure required to implement child protection mechanisms, such as age verification and parental consent mechanisms.

Two of the countries surveyed have plans to introduce legislation to protect children online. **Spain's** LPDP requires the government to draft a bill specifically designed to protect the rights of children online, but this has yet to be submitted to Congress. **France** is currently working on a detailed legal framework and practical advice to protect the rights of minors online and aims to issue its responses to a public consultation in mid-2021. **Germany** has recently approved an amendment to the Youth Protection Act, which will enter into force on May 1, 2021, and places a burden on providers of internet services aimed at or used by children to establish "adequate and effective structural preventive measures to enable children and adolescents to participate online in a carefree manner." This requires the use of stringent default settings that protect children from a number of issues, such as hate speech, excessive gaming and online tracking, and obligates providers to develop and implement age verification systems and support mechanisms for young audiences. Domestic providers with less than one million users are exempt from the requirements. Internet services that fail to comply with these obligations may be fined up to $60 million.

Denmark, Greece, Portugal, Sweden, Romania, and the **UK** do not currently have any future plans to further legislate on children's online privacy issues.

European Union

Jenny Gesley
Foreign Law Specialist

SUMMARY The data protection legal framework in the European Union (EU) currently consists of two main pillars, the Directive on Privacy and Electronic Communications (ePrivacy Directive) and the General Data Protection Regulation (GDPR). The GDPR contains specific rules governing consent to data processing when "information society services" are offered directly to children. Controllers of data are obligated to make reasonable efforts to verify that consent was given by the holder of parental responsibility.

In addition, the *EU Strategy for a More Effective Fight Against Child Sexual Abuse* is meant to ensure that existing EU rules are fully implemented and that possible gaps in the current legal framework are addressed, such as the role of online service providers. In September 2020, the European Commission published a proposal for an interim regulation that would temporarily derogate from certain provisions of the e-Privacy Directive to ensure that providers of online communications services can continue their voluntary practices to detect and report child sexual abuse online and remove child sexual abuse material.

The EU's Audiovisual Media Services Directive (AVMSD) obligates video-sharing platforms to take appropriate measures to protect minors from advertisements which may impair their physical, mental, or moral development and prohibits commercial communications for alcoholic beverages aimed specifically at minors and advertisements that cause physical, mental, or moral detriment to minors.

I. Introduction

The protection of personal data and the respect for private life are fundamental rights in the European Union (EU).[1] Personal data is defined as "any information relating to an identified or identifiable natural person (data subject)."[2] The data protection legal framework in the EU currently consists of two main pillars, the Directive on Privacy and Electronic Communications (ePrivacy Directive)[3] and the General Data Protection Regulation (GDPR).[4] The ePrivacy Directive is slated to be replaced by an ePrivacy Regulation; however, the legislative process is still ongoing as the discussions were stalled for several years. On January 5, 2021, the Portuguese

[1] Charter of Fundamental Rights of the European Union (EU Charter) arts. 7, 8, 2012 O.J. (C 326) 391, https://perma.cc/PAX8-4MYJ; Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 16, para. 1, 2016 O.J. (C 202) 1, https://perma.cc/GPB6-64TG.

[2] General Data Protection Regulation (GDPR), art. 4, point (1), 2016 O.J. (L 119) 1, https://perma.cc/7T85-89ZQ.

[3] Consolidated Version of the Directive on Privacy and Electronic Communications (ePrivacy Directive), 2002 O.J. (L 201) 37, https://perma.cc/YHA5-EFXV.

[4] GDPR, supra note 2.

Presidency of the Council released a new draft version of the proposed ePrivacy Regulation and a new mandate for negotiations was agreed on in February 2021.[5]

A. General Data Protection Regulation

As a regulation, the GDPR is directly applicable in the EU Member States with generally no domestic implementing legislation needed.[6] Processing of personal data[7] according to the GDPR must comply with the principles of lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy and keeping data up to date; storage limitation; and integrity and confidentiality.[8] Article 6 of the GDPR sets out the conditions under which data processing is considered lawful, with the most common ground being consent given by the data subject.[9]

B. ePrivacy Directive

The aim of the ePrivacy Directive is to ensure an equivalent level of protection of fundamental rights and freedoms (particularly the right to privacy) with respect to data processing in the electronic communications sector and to ensure the free movement of such data.[10] Directives must be transposed into national law and are binding with regard to their goals; the means are up to the Member States.[11] The ePrivacy Directive covers the processing of personal data by traditional telecom providers in public communications networks in the EU and mandates that Member States protect the confidentiality of the content of electronic communications through national legislation.[12] The proposed ePrivacy Regulation would extend coverage to internet-based voice and messaging services such as WhatsApp, Facebook Messenger, and Skype.[13]

---

[5] ePrivacy Regulation Proposal, COM(2017) 10 final (Jan. 10, 2017), https://perma.cc/N2WU-H2RL; *Legislative Train Schedule. Proposal for a Regulation on Privacy and Electronic Communication*, European Parliament (last updated Mar. 20, 2021), https://perma.cc/XQX9-SUQS.

[6] TFEU, art. 288, para. 2; GDPR, art. 99. Some provisions nonetheless require for their implementation the adoption of measures of application by the Member States—for example, the appointment of a national regulator and administrative sanctions for a violation of the GDPR. The GDPR also contains "opening clauses" that permit diverging national legislation in certain areas—for example, for the processing of special categories of personal data or in the context of employment.

[7] "Processing" means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR, art. 4, point (2).

[8] GDPR, art. 5, para. 1. For a more detailed overview, see Jenny Gesley, *Online Privacy Law: European Union* (Law Library of Congress, Dec. 2017), https://perma.cc/D36L-7EH8.

[9] GDPR, art. 6, para. 1(a), art. 7.

[10] ePrivacy Directive, art. 1, para. 1.

[11] TFEU, art. 288, para. 3.

[12] ePrivacy Directive, arts. 3, 5.

[13] ePrivacy Regulation Proposal, art. 18.

II. Data Protection for Children

A. General Data Protection Regulation

The GDPR contains specific rules governing consent to data processing when "information society services"[14] are offered directly to children.[15] If the child is younger than 16 years, parental consent is needed for the processing to be lawful. Member States may lower the age under which parental consent is needed to 13, and a number of Member States have set the age at 13, 14, or 15.[16] Controllers of data are obligated to make reasonable efforts to verify that consent was given by the holder of parental responsibility.[17] Because children are regarded as particularly vulnerable, any information or communication to a child has to be easily understandable in clear and plain language.[18]

Furthermore, the right to erasure ("right to be forgotten") under the GDPR provides data subjects with the right to require controllers to erase personal data when certain conditions are met.[19] Among other reasons, erasure may be demanded if the personal information has been collected in relation to the offer of information society services directly to a child and consent was given by the child, but he or she was not fully aware of the risks involved by the processing at the time, and later wants to remove such personal data.[20] This right may be exercised even if the data subject is no longer a child.[21]

The GDPR calls upon EU Member States, their supervisory authorities, the European Data Protection Board (EDPB), and the European Commission to encourage the drawing up of Codes of Conduct for the proper application of the GDPR.[22] One example mentioned are Codes of Conduct regarding "information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained."[23] National accredited competent bodies perform compliance with the Codes of Conduct.[24] Member

[14] "Information society services" are defined as services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. See Single Market Transparency Directive, art. 1(b), 2015 O.J. (L 241) 1, https://perma.cc/SQ86-5563.

[15] GDPR, art. 8, para. 1.

[16] Eight Member States opted for 13 years, six for 14 years, and three for 15 years (as of 2020). See SWD(2020) 115 final, at 17 (June 24, 2020), https://perma.cc/5HSH-3S9B.

[17] GDPR, art. 8, para. 2.

[18] Id. art. 12, para. 1, recital 58.

[19] Id. art. 17.

[20] Id. art. 17, para. 1(f), recital 65.

[21] Id. recital 65.

[22] Id. art. 40.

[23] Id. art. 40, para. 2(g).

[24] Id. art. 41.

States' supervisory authorities must raise public awareness of the risks, rules, and safeguards of data processing, and pay special attention to activities addressed directly to children.[25]

B. EU Strategy for a More Effective Fight Against Child Sexual Abuse

In addition, the *EU Strategy for a More Effective Fight Against Child Sexual Abuse* (EU Strategy) includes eight initiatives to put in place a strong legal framework for the protection of children online and offline.[26] The EU Strategy is meant to ensure that existing EU rules are fully implemented, especially the Directive on Combating Sexual Abuse and Exploitation of Children,[27] and that possible gaps in the current legal framework are addressed, such as the role of online service providers. In particular, the EU Strategy states that the European Commission will propose "legislation to tackle child sexual abuse online effectively including by requiring relevant online services providers to detect known child sexual abuse material and require them to report that material to public authorities" in the second quarter of 2021.[28]

In addition, the EU Strategy points out an unintended consequence that resulted from the application of the European Electronic Communications Code (EECC) on December 21, 2020.[29] The EECC made certain online communication services, like webmail or messaging services, subject to the e-Privacy Directive and its rules on confidentiality of communications and conditions for processing of data by expanding the definition of "electronic communications services."[30] Unlike the GDPR, the ePrivacy Directive does not contain an explicit legal basis for voluntary processing of content or traffic data for the purpose of detecting child sexual abuse online. As a result, providers of online communications services have to discontinue their voluntary practices to detect and report child sexual abuse online and remove child sexual abuse material unless EU Member States adopt specific national legislative measures according to article 15 of the ePrivacy Directive. Article 15 allows Member States to adopt national legislation that limits the scope of the ePrivacy Directive to prevent, investigate, detect, and prosecute criminal offenses, among other reasons.

In September 2020, the European Commission therefore published a proposal for an interim regulation to ensure that providers of online communications services can continue their voluntary practices.[31] The proposed regulation would temporarily derogate from certain provisions of the e-Privacy Directive and would cease to apply in December 2025 at the latest.[32]

---

[25] Id. art. 57, para. 1(b).

[26] EU Strategy for a More Effective Fight Against Child Sexual Abuse (EU Strategy), COM(2020) 607 final (July 24, 2020), https://perma.cc/SMV6-QU5X.

[27] Directive 2011/93/EU, 2011 O.J. (L 335) 1, https://perma.cc/EM9S-4N4S.

[28] EU Strategy, supra note 26, at 6.

[29] Id. at 4.

[30] European Electronic Communications Code, art. 2 (4), 2018 O.J. (L 321) 36, https://perma.cc/H3TH-6PUN.

[31] Proposal for a Regulation on a Temporary Derogation from Certain Provisions of Directive 2002/58/EC, COM(2020) 568 final (Sept. 10, 2020), https://perma.cc/Z6AB-JXM6.

[32] The proposal would allow a temporary derogation from art. 5, para. 1, and art. 6 of the ePrivacy Directive.

The legislative process is still ongoing.[33] However, the voluntary practices must meet GDPR requirements and concerns have been raised with regard to their compliance.[34]

III. Advertisements on Platforms Designed for Children

One of the goals of the EU's Audiovisual Media Services Directive (AVMSD) is to protect children and consumers.[35] Audiovisual media services include both traditional TV broadcasts and on-demand audiovisual media services. Since an amendment of the AVMSD in 2018, it also covers video-sharing platforms and audiovisual content shared on certain social media services.[36] The AVMSD is supplemented by a 1998 Recommendation and 2006 Recommendation on the protection of minors and human dignity with a focus on online services.[37] Furthermore, the European Commission has issued a communication that specifies the definition of "video-sharing platform."[38]

Under the AVMSD, video-sharing platforms must take appropriate measures to protect minors from audiovisual commercial communications that may impair their physical, mental, or moral development, whereby the most harmful content must be subject to the strictest access control measures. Such measures are age-verification systems or parental control systems, among others.[39] Furthermore, EU Member States must encourage the adoption of Codes of Conduct for video-sharing platforms to reduce the exposure of children to audiovisual commercial communications for unhealthy foods and beverages.[40]

The AVMSD prohibits audiovisual commercial communications for alcoholic beverages aimed specifically at minors.[41] Member States should encourage the adoption of Codes of Conduct to limit the exposure of children to alcoholic beverage advertisements.[42] Furthermore,

---

[33] See Procedure File on 2020/0259 (COD), Use of Technologies by Number-independent Interpersonal Communications Service Providers for the Processing of Personal and Other Data for the Purpose of Combatting Child Sexual Abuse Online (Temporary Derogation from Certain Provisions of Directive 2002/58/EC), Legislative Observatory European Parliament, https://perma.cc/N3GU-3T5C.

[34] *Legislative Train Schedule. Proposal for a Regulation on a Temporary Derogation from Certain Provisions of the ePrivacy Directive for the Purpose of Combating Child Sexual Abuse Online*, European Parliament (last updated Mar. 20, 2021), https://perma.cc/BX7Y-4HCB.

[35] Consolidated Version of Audiovisual Media Services Directive (AVMSD), 2010 O.J. (L 95) 1, https://perma.cc/8T3W-SNG3. Original Version of AVMSD, recital 104, 2010 O.J. (L 95) 1, https://perma.cc/JE3P-PNHL.

[36] AVMSD, art. 1, paras. 1(a), 1(aa).

[37] Council Recommendation 98/560/EC, 1998 O.J. (L 270) 48, https://perma.cc/K55Y-J2DG; Recommendation 2006/952/EC of the European Parliament and of the Council, 2006 O.J. (L 378) 72, https://perma.cc/X8H9-UJ6X.

[38] Communication from the Commission, 2020 O.J. (C 223) 3, https://perma.cc/X6RZ-9YQW.

[39] AVMSD, art. 28b, paras. 1, 3.

[40] Id. art. 28b, paras. 2, 3.

[41] Id. art. 9, para. 1(e).

[42] Id. art. 9, para. 3.

advertisements may also not cause physical, mental, or moral detriment to minors, meaning "they shall not directly exhort minors to buy or hire a product or service by exploiting their inexperience or credulity, directly encourage them to persuade their parents or others to purchase the goods or services being advertised, exploit the special trust minors place in parents, teachers or other persons, or unreasonably show minors in dangerous situations."[43]

It is prohibited to process personal data of minors collected or otherwise generated by media service providers and video-sharing platforms to prevent showing harmful content to minors for commercial purposes, such as direct marketing, profiling and behaviorally targeted advertising.[44]

IV. Future Plans to Protect Children Online

As mentioned above, the European Commission will propose legislation to tackle child sexual abuse online in the second quarter of 2021.[45]

In addition, the EU has published a call for proposals for a pilot project to "demonstrate an interoperable technical infrastructure dedicated to the implementation of child protection mechanisms (such as age verification) and parental consent mechanisms based on relevant EU legislation such as the AVMSD and GDPR."[46]

[43] Id. art. 9, para. 1(g).

[44] Id. art. 6a, para. 2, art. 28b, para. 3 at the end.

[45] See note 28.

[46] European Commission, *Pilot Project. Call for Proposals Document* (June 15, 2020), https://perma.cc/A2MP-R7JL.

Denmark

Elin Hofverberg
Foreign Law Specialist

SUMMARY The right to privacy is constitutionally protected in Denmark. As Denmark is a member of the European Union, the General Data Protection Regulation applies directly. The age for legal consent to data processing is set at 13 years. The Data Protection Authority has issued guidelines providing that the processing of data pertaining to children always warrants an impact assessment.

Advertisements that target children, both offline and online, must be clearly identifiable as advertisements to the child. Such advertisements may not promote violence. Advertisements of tobacco products, including e-cigarettes, targeting children are specifically prohibited. The Consumer Ombudsman has found that sending products to underaged influencers intending that they promote the products online constitutes hidden advertising and is prohibited.

There are no bills regarding children's privacy protection online pending before parliament.

I. Introduction

The Danish Constitution protects the right to privacy.[1] Denmark is a member of the European Union (EU), and the General Data Protection Regulation (GDPR) is automatically applicable there; implementing legislation was not required.[2] At the time of entry into force of the GDPR, on May 25, 2018, additional rules regarding data protection were enacted in a new Data Protection Act.[3] Denmark has also implemented the ePrivacy Directive.[4] As specified in the Data Protection Act, the Data Protection Authority oversees compliance with the GDPR and the ePrivacy Directive.[5] Thus, the Data Protection Authority may issue fines for violating the GDPR.[6]

[1] § 72 Grundloven (LOV nr 169 af 05/06/1953), https://perma.cc/62DH-W7W6.

[2] General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1, https://perma.cc/JG59-NUXN.

[3] Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (Databeskyttelsesloven) (LOV nr 502 af 23/05/2018), https://perma.cc/83RT-CXKU.

[4] Lov om ændring af lov om elektroniske kommunikationsnet og -tjenester, lov om radiofrekvenser og forskellige andre love (LOV nr 1833 af 08/12/2020), https://perma.cc/T6E9-5JLN, implementing Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, 2018 O.J. (L 321, 36) (Consolidated).

[5] § 2 Databeskyttelsesloven.

[6] GDPR art. 83; §§ 39-44 Databeskyttelsesloven.

The Authority has issued a guide on the issuance of fines in relation to the GDPR.[7] As prescribed in GDPR article 83.1, the fine must be "effective, proportionate and dissuasive."[8] The Data Protection Authority guide explains how the fines must first be determined using a benchmark value, which is then adjusted to reflect "the circumstances the art of the infringements, and the seriousness and duration."[9] Violations regarding the consent of children are considered among the most serious infringements, and the standard bench value will be set to 20% of the maximum fine before issues such as seriousness and duration are considered,[10] which is DKK 15 million (about US$2.4 million).[11] For smaller organizations, the standard bench value for violations against children may be reduced, but not to less than DKK 60,000 (about US$10,000).[12]

II. Data Protection for Children

As provided for in the GDPR, children may consent to data processing in accordance with member state legislation. Under the Data Protection Act, children in Denmark must be at least 13 years old to consent to the processing of their personal data.[13] If the child is not old enough to consent, a parent may consent on the child's behalf.[14]

The Danish Data Protection Authority has issued guidelines regarding the use of personal data from visitors to individual websites.[15] However, these rules do not specifically address children's rights or protections.[16] The Data Protection Authority's guidance on article 35 of the GDPR also does not specifically mention children, but provides guidance pertaining to "vulnerable groups," which includes children.[17] The guidance says the processing of data pertaining to these groups always warrants an impact assessment.[18]

---

[7] Datatilsynet, *BødevejledningUdmåling af bøder til virksomheder* (Jan. 2021), https://perma.cc/RK48-U54U.

[8] GDPR art. 83.1.

[9] Datatilsynet, *BødevejledningUdmåling af bøder til virksomheder*, supra note 7, at 10.

[10] Id. at 6-7.

[11] Id. at 8.

[12] Id.

[13] § 6 stk 2 Databeskyttelsesloven.

[14] Id. § 6 stk 3.

[15] Dattilsynet, *Vejledning - Behandling af personoplysninger om hjemmesidebesøgende* (Feb. 2020), https://perma.cc/22L4-N3R9.

[16] Id.

[17] Dattilsynet, Datatilsynets liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse jf. databeskyttelsesforordningens artikel 35, stk. 4, https://perma.cc/2GYK-VCQW.

[18] Id.

In 2021, the Data Protection Authority issued serious criticism of a firm called Epic Bookings for violating the GDPR by publishing pictures of children on its website without sufficient consent.[19] The Data Protection Authority noted that although the children aged 14 and up had consented to some uses of the pictures, the company used them for other purposes for which the children did not specifically and voluntarily provide consent.[20] In addition, the Data Protection Authority seriously criticized Epic Bookings for not providing a time limit for how long the pictures would be used, a clear violation of the GDPR.[21]

III. Advertisements on Platforms Designed for Children

Recital 38 of the GDPR provides that the use of personal data of children for marketing purposes requires additional safeguards.[22] Marketing rules in Denmark are based on good practice and custom.[23] Advertisements that directly target children "must be designed with special consideration to the child or youth's natural credulity and lack of experience and critical sense, which means that they are easier to influence and impress."[24] Specifically, all advertisements to minors of tobacco products, including non-tobacco e-cigarettes, are prohibited.[25] Similarly, advertisements targeting children may not promote violence.[26] Per the Consumer Ombudsman's guidance, advertisements online must be identifiable as advertisements, and designed with the youngest audience in mind.[27] In 2020, the Consumer Ombudsman declared that it violated Danish law for a cosmetic company to send products to a 13-year-old social media influencer so that the child would post about the products on the child's social media accounts, as it constituted hidden advertising.[28]

[19] Datatilsynet, Epic Bookings behandling af personoplysninger (Mar. 1, 2021), https://perma.cc/5ZQM-ZMDD.

[20] Id.

[21] Id.

[22] GDPR recital 38.

[23] Lov om markedsføring (LOV nr 426 af 03/05/2017), https://perma.cc/XK6B-7A2A.

[24] Id. § 3.

[25] § 11 Lov om markedsføring; § 2 Bekendtgørelse om forbud mod reklame, synlig anbringelse og fremvisning m.v. af elektroniske cigaretter og genopfyldningsbeholdere med og uden nikotin (BEK nr 65 af 15/01/2021), https://perma.cc/CL4Y-T47P.

[26] § 11 Lov om markedsføring.

[27] Forbrugerombudsmanden, *Gode råd til influenter om skjult reklame* 6, https://perma.cc/W27N-VBPN; *Markedsføring over for børn og unge*, Forbrugerombudsmanden, https://perma.cc/6NSM-CCQ8.

[28] Forbrugerombudsmanden, *Ulovligt at bruge barns SoMe-profil til markedsføring* (June 18, 2020), https://perma.cc/S6PH-D2A5.

IV. Future Plans to Protect Children Online

There are currently no pending proposals in the Danish Parliament to increase the protection of children's privacy protections online.

France

Nicolas Boring
Foreign Law Specialist

SUMMARY Data protection in France is principally governed by the European Union General Data Protection Regulation and by the domestic Law on Information Technology and Freedoms (*Loi Informatique et Libertés*). Personal data must be processed lawfully and fairly, and must not be used in a manner that is incompatible with the explicit and legitimate purposes for which it was collected. Mishandling personal data in or through a computerized system is punishable under the French Penal Code. Data protection rules are enforced by an independent agency called the National Commission on Information Technology and Freedoms (*Commission nationale de l'informatique et des libertés*), referred to by its French acronym, CNIL. The CNIL also provides advisory opinions to the government and informs the public on data privacy issues.

The Law on Information Technology and Freedoms provides that minors may consent to the processing of their personal data only if they are 15 years old or older. Younger children may consent to the processing of their personal data only if their parents or legal guardians also consent. The processor must write the information and communications regarding the processing of the child's data in terms that are clear, simple, and easily understood by a child. Currently, there do not appear to be any other specific rules regarding data protection for children, but the CNIL is in the process of drafting a more detailed legal framework as well as practical advice to better protect the rights of minors online.

I. Introduction

The French Civil Code provides that everyone has a right to privacy.[1] However, data protection in France is primarily governed by the European Union (EU) General Data Protection Regulation (GDPR), and by the domestic Law on Information Technology and Freedoms (*Loi Informatique et Libertés*).[2] The latter was originally adopted in 1978, but has been amended many times since. For example, it was amended in 2004 to incorporate provisions from the EU's ePrivacy Directive,[3] and it was amended in 2018 to be consistent with the GDPR and EU Directive 2016/680 on the processing of personal data.[4]

[1] Code civil art. 9, https://perma.cc/UPQ8-MH6K.

[2] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (as amended) (Loi Informatique et Libertés), https://perma.cc/ZW2C-R6QN.

[3] Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Aug. 6, 2004), https://perma.cc/FPZ7-DBA6.

[4] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (June 20, 2018), https://perma.cc/2Y25-G7ZW; Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification

The Law on Information Technology and Freedoms states that information technology "should not infringe upon human identity, human rights, privacy, or public or individual freedoms."[5] Personal data must be processed lawfully and fairly, and data that falls under the GDPR should be processed in a manner that is also transparent for the data subject.[6] Data may not be used in a manner that is incompatible with the explicit and legitimate purposes for which it was collected.[7]

Mishandling personal data in or through a computerized system, whether intentionally or by negligence, is punishable under the French Penal Code.[8] Someone who violates the rules set out in the GDPR or the Law on Information Technology and Freedoms can be sentenced to a fine of up to 300,000 Euros (about US$361,400) and up to five years in jail.[9]

The Law on Information Technology and Freedoms set up the National Commission on Information Technology and Freedoms (*Commission nationale de l'informatique et des libertés*, CNIL), an independent agency tasked with enforcing regulatory or legislative texts regarding the use of personal data.[10] The CNIL also provides advisory opinions to the government and informs the public about data privacy issues.[11]

II. Data Protection for Children

A. Consent Requirements

In applying article 8 of the GDRP, the Law on Information Technology and Freedoms provides that minors may consent to the processing of their personal data only if they are 15 years old or older.[12] Children under the age of 15 may only consent to the processing of their personal data if their parents or legal guardians also consent to it.[13] The processor must write the information and communications regarding the processing of the child's data in terms that are clear, simple, and easily understood by a child.[14] Similarly, under article 13 of the GDPR, the information to be provided where personal data are collected from a child aged 15 or younger must be clear and easily understood.[15]

---

de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel (Dec. 12, 2018), https://perma.cc/7U58-XB42.

[5] Loi Informatique et Libertés art. 1.

[6] Id. art. 4.

[7] Id.

[8] Code pénal arts. 226-16 to 226-24, https://perma.cc/UCG5-CHKV.

[9] Id.

[10] Loi Informatique et Libertés art. 8.

[11] Id.

[12] Loi Informatique et Libertés art. 45.

[13] Id.

[14] Id.

[15] Id. art. 48.

B. Data Protection

Beyond these provisions, currently there do not appear to be any specific rules regarding data protection for children. Rather, the same rules that apply to adults would apply to children.

As a general rule, data may not be retained in a manner that allows the data subjects' identification beyond the time necessary to fulfill the purpose for which it was collected.[16] The main exception is that data, even personal information, may be retained for archival purposes, for historical or scientific research, or for statistical purposes. Even within this exception, however, the data must be kept in a manner that complies with the GDPR, and it may not be used to make decisions concerning the data subjects.[17] Additionally, data must be kept in a manner that adequately protects personal information from being lost, destroyed, damaged, or used in an illegal or unauthorized manner.[18]

Data that is found to be inaccurate with regard to the purpose for which it was collected should be immediately corrected or erased.[19] Additionally, data subjects have a right to demand that their personal data be erased.[20] Furthermore, the CNIL has the authority to demand that data be rectified or erased if it finds that the GDPR or other legal requirements have not been respected.[21]

C. Official Guidance

There does not yet appear to be official guidance on the specifics of implementing the digital privacy rights of children. However, the CNIL is currently in the process of elaborating a more detailed legal framework as well as practical advice to better protect the rights of minors online.[22] The CNIL organized a public consultation on this topic from April to June 2020, and it is expected to issue its conclusions by the middle of 2021.[23]

III. Advertisements on Platforms Designed for Children

While television advertisements aimed at children are regulated,[24] there does not appear to be any specific legislation or regulation regarding online advertising designed for children.

---

[16] Id. art. 4.

[17] Id.

[18] Id.

[19] Id.

[20] Id. arts. 51, 106.

[21] Id. art. 20.

[22] CNIL, *Droits Numériques des Mineurs: La CNIL Publie les Résultats du Sondage et de la Consultation Publique* (Jan. 11, 2021), https://perma.cc/AKU7-F6CM.

[23] Id.

[24] Décret n°87-239 du 6 avril 1987 pris pour l'application de l'article 27-I de la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication et fixant pour les services privés de radiodiffusion sonore diffusés par voie hertzienne terrestre ou par satellite le régime applicable à la publicité et au parrainage (as amended), https://perma.cc/KE9V-B3DA.

IV. Future Plans to Protect Children Online

As mentioned above, the CNIL is currently engaged in a project to provide a more detailed legal framework and guidance regarding children's online privacy. Apart from this project, there currently do not appear to be any other plans on this issue in France.

Germany

Jenny Gesley
Foreign Law Specialist

SUMMARY The right to informational self-determination and the right to confidentiality and integrity of information technology systems are constitutionally guaranteed in Germany. The data protection legal framework consists of the directly applicable European Union General Data Protection Regulation (GDPR) and the German Federal Data Protection Act, which supplements the GDPR. The GDPR contains special rules for consent to data processing when "information society services" are offered directly to children.

German law prohibits advertisements that directly exhort children to purchase the goods or services marketed or to persuade their parents or other adults to do so, as well as those that exploit their young age or inexperience. In general, advertisements may not harm the physical or mental development of children. Advertisements for alcoholic beverages aimed specifically at minors are prohibited. Service providers must take appropriate measures to reduce the exposure of children to advertisements for unhealthy foods.

An amendment to the Youth Protection Act, which will enter into force on May 1, 2021, will obligate providers of internet services that are aimed at or used by children to set up preventive measures to enable children and adolescents to "participate online in a carefree manner." Such measures are age-appropriate default settings, age-verification systems, and support and complaint mechanisms suitable for a young target audience.

I. Introduction

The right to informational self-determination is constitutionally guaranteed in Germany.[1] Informational self-determination guarantees the right of individuals to decide which personal data they would like to disclose and how such data will be used.[2] In addition, with regard to online protection of personal data, the German Basic Law (Constitution) protects the basic right to confidentiality and integrity of information technology systems ("IT basic right").[3] It ensures "that the data which are created, processed and stored by the information technology system that

[1] Grundgesetz für die Bundesrepublik Deutschland [Grundgesetz] [GG], May 23, 1949, Bundesgesetzblatt [BGBl.] I at 1, as amended, art. 2, para. 1 in conjunction with art. 1, para. 1, https://perma.cc/4JK9-TYXG (original), https://perma.cc/6FCR-JZZP (English translation, updated through Mar. 28, 2019).

[2] Bundesverfassungsgericht [BVerfG], Dec. 15, 1983, Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 65, 1, para. 147, https://perma.cc/3T5W-GA7A (original), https://perma.cc/B52M-CTSU (English abstract).

[3] GG, art. 2, para. 1 in conjunction with art. 1, para. 1; BVerfG, BVerfGE 120, 274, paras. 166, 201, https://perma.cc/42A4-THNJ (original), https://perma.cc/3U9C-LUDH (English translation).

is covered by its scope of protection remain confidential."[4] Furthermore, article 5, paragraph 2 of the Basic Law requires that legal provisions for the protection of young people be enacted.

The European Union (EU) General Data Protection Regulation (GDPR)[5] is directly applicable in Germany with, generally, no domestic implementing legislation needed.[6] However, the GDPR also contains "opening clauses" that permit derogations for national legislation in certain areas,[7] and it specifically allows EU Member States to incorporate elements of the GDPR into their national law as far as necessary for coherence and comprehensibility.[8] Germany therefore published the amendment of its Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) in July 2017.[9] It entered into force at the same time as the GDPR started applying in Germany, on May 25, 2018. The ePrivacy Directive of the EU, which aims to ensure an equivalent level of protection of fundamental rights and freedoms (particularly the right to privacy) with respect to data processing in the electronic communications sector, was transposed in the German Telecommunications Act (Telekommunikationsgesetz, TKG).[10]

The new German Federal Data Protection Act focuses on the areas for which the GDPR contains "opening clauses" allowing Member States to initiate more restrictive provisions, as the other areas are governed by the provisions of the GDPR itself.[11] It also has a wider scope than the GDPR; it applies to the processing of personal data by federal and state public authorities and bodies as well as by private bodies.[12]

---

[4] BVerfG, para. 204.

[5] General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1, https://perma.cc/7T85-89ZQ.

[6] Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 288, para. 2, 2016 O.J. (C 202) 1, https://perma.cc/GPB6-64TG. Some provisions nonetheless require for their implementation the adoption of application measures by the Member States—for example, the appointment of a national regulator and administrative sanctions for a violation of the GDPR.

[7] GDPR, recitals 10, 19, 52; art. 9, para. 4; art. 88.

[8] Id. recital 8.

[9] Bundesdatenschutzgesetz [BDSG], June 30, 2017, BGBl. I at 2097, https://perma.cc/74U7-UR8M (original), https://perma.cc/E827-452T (English translation).

[10] Telekommunikationsgesetz [TKG], June 22, 2004, BGBl. I at 1190, as amended, https://perma.cc/3JUK-3BXK. For a detailed overview of the ePrivacy Directive, see the EU survey in this report.

[11] The new German Federal Data Protection Act took advantage of the opening clauses related to collection and use of employee data (§ 26), special categories of data (sensitive data) (§ 22), processing of data for research purposes and statistical purposes (§ 27), processing for archiving purposes in the public interest (§ 28), processing for other purposes than the ones for which the personal data have been originally collected (§ 24), restrictions on the investigative power of data protection authorities in cases of professional secrecy (§ 29, para. 3), appointment of data protection officers (§ 38), consumer loans (§ 30), credit reports and scoring (§ 31), sanctions (§§ 41-43), the right of data protection authorities to file an action against a decision of the EU Commission (§ 21), video surveillance (§ 4), and restrictions on some of the data subjects' rights (§§ 32–37).

[12] BDSG, § 1; GDPR, recital 19.

The processing of personal data,[13] according to the GDPR, must comply with the principles of lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy and keeping data up to date; storage limitation; and integrity and confidentiality.[14] Article 6 of the GDPR sets out the conditions under which data processing is considered lawful, with the most common ground being consent given by the data subject.[15]

II. Data Protection for Children

Among other things, the German Federal Data Commissioner is tasked with promoting public awareness and understanding of the risks, rules, safeguards, and rights in relation to the processing of personal data, and must pay special attention to measures addressed specifically to children.[16]

The GDPR contains specific rules governing consent to data processing when "information society services"[17] are offered directly to children.[18] If the child is younger than 16 years, parental consent is needed for the processing to be lawful. Germany did not make use of the option to lower the age of consent. Controllers of data are obligated to make reasonable efforts to verify that consent was given by the holder of parental responsibility.[19] It appears that the German data protection authorities have published no official guidance on how this GDPR requirement should be implemented.

However, a case decided by the German Federal Court of Justice (Bundesgerichtshof, BGH) in 2007 that involved age-verification systems for accessing pornographic websites might provide some insight.[20] The court held that requiring users to enter their national ID or passport number and the zip code of the city where the identity document was issued was insufficient. Entering a name, address, and credit card or bank account information and paying a minor amount in addition was equally insufficient. In the opinion of the Federal Court of Justice, these were not effective entry barriers, because children could easily get ahold of the ID or passport number of

[13] "Processing" means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR, art. 4, point (2).

[14] Id. art. 5, para. 1. For a more detailed overview, see Jenny Gesley, *Online Privacy Law: European Union*, Law Library of Congress (Dec. 2017), https://perma.cc/D36L-7EH8.

[15] GDPR art. 6, para. 1(a), art. 7.

[16] BDSG § 14, para. 1, no. 2.

[17] "Information society services" are defined as services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. See Single Market Transparency Directive, art. 1(b), 2015 O.J. (L 241) 1, https://perma.cc/SQ86-5563.

[18] GDPR art. 8, para. 1.

[19] Id. art. 8, para. 2.

[20] BGH, Oct. 18, 2007, docket no. I ZR 102/05, https://perma.cc/EU64-YUQ4.

an adult and oftentimes had their own bank accounts.[21] As alternative age-verification systems, the court listed ones recommended by the Commission for Youth Media Protection (Kommission für Jugendmedienschutz (KJM),[22] in particular a one-time in-person identification, such as PostIdent;[23] an identification with a USB stick and a pin code every time the user logs on; or identification by technical means, such as a webcam or recognition of biometrical features.[24]

III. Advertisements on Platforms Designed for Children

German law provides special rules for advertisements geared towards children. These rules apply on all types of platforms, not just those designed for children. The German Act Against Unfair Competition (Gesetz gegen den unlauteren Wettbewerb, UWG) prohibits unfair commercial practices.[25] Among other things, commercial practices that are always considered unfair and therefore illegal are advertisements that directly exhort children to purchase the goods or services marketed or to persuade their parents or other adults to do so.[26] In addition, there is a prohibition on exploiting their young age or inexperience to cause them to make a transactional decision that they would not have made otherwise (aggressive commercial practices).[27]

The Interstate Treaty on the Protection of Minors in the Media (Jugendmedienschutz-Staatsvertrag, JMStV) contains additional requirements for advertisements geared towards children and adolescents.[28] It implements the requirements of the EU's Audiovisual Media Services Directive (AVMSD).[29] Video-sharing platforms must take appropriate measures to protect minors from offers that may impair their development, such as using age-verification systems or parental control systems.[30] In general, advertisements may not physically or mentally harm children and may not

1. directly exhort minors to buy or hire a product or service by exploiting their inexperience or credulity,

[21] Id. para. 30.

[22] Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien [Jugendmedienschutz-Staatsvertrag] [JMStV], Sept. 10-27, 2002, Gesetz-und Verordnungsblatt Bayern [GVBl. Bayern] 2003 at 147, as amended, § 14, https://perma.cc/86PK-MCM4.

[23] PostIdent is a method of secure personal identification of a person by an employee of the German post office.

[24] BGH, paras. 34, 35. For a list of positively evaluated age-verification systems, see *Technische Mittel*, KJM, https://perma.cc/9Z2N-UBU8. See also Press Release, KJM, *KJM bewertet sechs weitere Altersverifikationssysteme positiv* (Apr. 13, 2021), https://perma.cc/6VPX-7J5D.

[25] Gesetz gegen den unlauteren Wettbewerb [UWG], Mar. 3, 2010, BGBl. I at 254, as amended, § 3, para. 1, https://perma.cc/EM59-LPC3 (original), https://perma.cc/PBU6-3JRG (English translation, updated through Apr. 18, 2019).

[26] Id. § 3, para. 1 in conjunction with annex, no. 28.

[27] Id. § 4a, para. 1, sentence 1, sentence 2, no. 3 in conjunction with § 4a, para. 2, sentence 1, no. 3, sentence 2.

[28] JMStV, supra note 22.

[29] Consolidated Version of Audiovisual Media Services Directive (AVMSD), 2010 O.J. (L 95) 1, https://perma.cc/8T3W-SNG3.

[30] JMStV § 5a.

2. directly encourage them to persuade their parents or others to purchase the goods or services being advertised,
3. exploit the special trust minors place in parents, teachers or other persons, or
4. unreasonably show minors in dangerous situations.[31]

Furthermore, advertisements for alcoholic beverages aimed specifically at minors are prohibited, as are those that appeal to minors or show them consuming alcohol.[32] Service providers must take appropriate measures to reduce the exposure of children to advertisements accompanying or included in children's programs, for foods containing nutrients and substances with a nutritional or physiological effect, in particular fat, trans-fatty acids, salt, sodium, and sugars, of which excessive intakes in the overall diet are not recommended.[33]

IV. Future Plans to Protect Children Online

On March 26, 2021, the German Bundesrat, the legislative body through which the German states participate in the legislative process, approved an amendment to the Youth Protection Act that the German Bundestag (parliament) passed on March 5, 2021.[34] The amendment will enter into force on May 1, 2021.[35]

The explanatory memorandum to the draft act states that the amendment was necessary because of changes in media usage by children and adolescents, and to cover risks that are associated with online interactions.[36] The amendment specifies requirements for advertisements and other content shown to young people. The aims of children and youth protection in the media are protecting minors from content that impairs or is harmful to their development, protecting their personal integrity, and promoting media literacy.[37] Significant risks to their personal integrity may arise from communication and contact functions, purchasing options, gambling-like mechanisms, mechanisms to encourage excessive media usage, disclosure of user data without consent to third parties, and age-inappropriate exhortation of minors to buy a product or service, in particular advertisements for third party services, among others.[38]

[31] Id. § 6, para. 2.

[32] Id. § 6, para. 5.

[33] Id. § 6, para. 7.

[34] Deutscher Bundesrat: Drucksachen und Protokolle [BR-Drs.] 195/21 (Beschluss), https://perma.cc/R46T-HK3Z; Jugendschutzgesetz [JuSchG], July 23, 2002, BGBl. I at 2730, as amended, https://perma.cc/3GHJ-K82X; Zweites Gesetz zur Änderung des Jugendschutzgesetzes, Apr. 9, 2021, BGBl. I at 742, https://perma.cc/9KUC-LAGD.

[35] Zweites Gesetz zur Änderung des Jugendschutzgesetzes art. 2.

[36] Deutscher Bundestag: Drucksachen und Protokolle [BT-Drs.] 19/24909, at 22, https://perma.cc/Q9VF-CYGQ (original), https://perma.cc/X73F-EHVK (English translation).

[37] Zweites Gesetz zur Änderung des Jugendschutzgesetzes art. 1, no. 3, § 10a.

[38] Id. art. 1, no. 3, § 10b, para. 3.

The explanatory memorandum states that

> [t]he media use of children and adolescents is today largely digital, mobile and interactive. They often unconsciously disclose a large amount of sensitive personal data, generate content themselves, are exposed to it and communicate with an almost indefinite group of people, often anonymously. They are potentially endangered in their personal integrity. Phenomena such as sexting, cybergrooming or cyberbullying pose dangers for children and adolescents who can limit their safe participation in digital media. But also phenomena such as the improper collection and use of personal data, the risk of an early and therefore comprehensive creation of an overall picture of children and adolescents (profiling), the promotion of excessive use and the exploitation of the business inexperience of children and adolescents, for example through cost traps, represent real danger. . . . [39]

Among other things, the amendment introduces the concept of "provider prevention" to enforce the goals of the law mentioned above. "Provider prevention" means that providers of internet services that are aimed at or used by children and adolescents will be obligated to set up "adequate and effective structural preventive measures to enable children and adolescents to participate online in a carefree manner."[40] For example, providers will have to install default settings that protect children and adolescents from mobbing, cyber grooming, self-endangering behavior, excessive gaming, cost traps,[41] hate speech, and tracking.[42] In addition, providers will be obligated to develop and implement adequate protection concepts such as age-appropriate default settings, age-verification systems, and support and complaint mechanisms suitable for their young target audience.[43] Noncompliance with service provider obligations carries administrative fines of up to 50 million euros (about US$60 million).[44] Service provider with less than one million users in Germany will be exempt from these requirements.[45] The obligations apply to domestic and foreign service providers.[46]

[39] BT-Drs. 19/24909, at 42 (44 in the English version).

[40] Zweites Gesetz zur Änderung des Jugendschutzgesetzes art. 1, no. 19, § 24a.

[41] Such as "loot boxes" in online games.

[42] BT-Drs. 19/24909, at 21.

[43] Zweites Gesetz zur Änderung des Jugendschutzgesetzes art. 1, no. 19, § 24a, para. 2.

[44] Id. art. 1, no. 23 in conjunction with Gesetz über Ordnungswidrigkeiten [OWiG], Feb. 19, 1987, BGBl. I at 602, as amended, § 30, para. 2, sentence 3, https://perma.cc/S2H6-6SA2 (original), https://perma.cc/4NUK-AASY (English translation, updated through June 21, 2019).

[45] Zweites Gesetz zur Änderung des Jugendschutzgesetzes art. 1, no. 19, § 24a, para. 3.

[46] Id. art. 1, no. 19, § 24a, para. 4.

Greece

Kayahan Cantekin
Foreign Law Specialist

SUMMARY The Constitution of Greece guarantees the "right to participate in the Information Society" and the right to protection of personal data against unauthorized collection, processing, and use. The Greek data protection framework consists of the European Union General Data Protection Regulation (GDPR) and the domestic implementation of relevant EU legislation. In accordance with the GDPR, Greece has opted to set the age of consent to data processing at 15 years. Greek law transposes the EU Audiovisual Media Services Directive's general restrictions concerning advertisements directed to minors, including those applicable to video-sharing platform services. The Greek advertising industry has adopted the Greek Code of Advertising-Communications (EKD-E), which is administered by the industry self-regulation organization, the Greek Advertising Self-Regulation Council. The EKD-E provides for certain rules and principles governing the format and content of advertisements directed to children and teenagers. There are presently no reports of future plans to amend the current framework regarding protection of the personal data of minors in Greek law.

I. Introduction

The Greek Constitution enshrines the right of all persons to information and guarantees "the right to participate in the Information Society."[1] Additionally, the Constitution requires the state to facilitate the access to electronically transmitted information and the "production, exchange and diffusion" of such information, subject to the constitutional guarantees of privacy of the home, privacy of correspondence, and the protection of personal data.[2] The right to protection against unauthorized collection, processing, and use of personal data is specifically guaranteed in article 9A of the Constitution. The Constitution also mandates the protection of childhood and youth in the state's regulation of radio and television.[3]

The European Union's (EU) General Data Protection Regulation (GDPR)[4] is directly applicable in Greece.[5] Certain measures provided by the GDPR require additional statutory implementation at the national level, and the GDPR allows the adoption into national law certain specifications or

[1] Constitution of the Greece (as revised by the parliamentary resolution of Nov. 25, 2019 of the IXth revisionary parliament) art. 5A(1), https://perma.cc/GUM8-V6KD.

[2] Id. arts. 9, 19, and 9A, respectively.

[3] Id. art. 15(2).

[4] General Data Protection Regulation (GDPR) 2016 O.J. (L 119) 1, https://perma.cc/7T85-89ZQ. For an overview of the EU legislation and an explanation of terms such as "information society services," and "data processing," see the EU survey in this report.

[5] Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 288, para. 2, 2016 O.J. (C 202) 1, https://perma.cc/GPB6-64TG.

restrictions provided in the Regulation as necessary for coherence or for making them comprehensible.[6] Accordingly, Law No. 4624/2019 was enacted to implement the GDPR, together with Directive (EU) 2016/680,[7] in Greek law.[8] The law entered into force with its publication in the Government Gazette on August 29, 2019.[9] The other major legislation of the Greek data privacy framework is Law No. 3471/2006, which transposes the EU's Directive 2002/58/EC (ePrivacy Directive).[10]

II. Data Protection for Children

In accordance with article 8 of the GDPR, Law No. 4626/2019 provides that minors that have reached the age of 15 may give consent to the processing of their personal data for lawful purposes when "information society services" are provided directly to them.[11] Any processing of personal data of minors younger than 15 years requires the consent of the minor's legal representative.[12] Law No. 4624/2019 also requires data controllers to use clear and concise wording in communications with minors about their rights as data subjects.[13]

The abovementioned rules are the only ones in the Greek data protection framework that specifically address the protection of minors' personal data in the provision of information society services.[14]

III. Advertisements on Platforms Designed for Children

Law No. 4779/2021 transposes the EU's Audiovisual Media Services Directive into Greek law, including its requirements for the protection of minors from certain types and methods of advertising on television and video-sharing platforms. The law generally prohibits commercial communications that (a) directly exhort minors to buy or hire a product or service by exploiting their inexperience or credulity, (b) encourage them to persuade their parents or others to purchase the goods or services being advertised, (c) exploit the special trust minors place in parents,

[6] GDPR recital 8.

[7] 2016 O.J. (L119) 89, https://perma.cc/AN84-RLDN (consolidated version).

[8] Law No. 4624/2019 (E.K.E.D. 2019, A:137), https://perma.cc/BQG8-8ZRK.

[9] Id. art. 87.

[10] Consolidated Version of the Directive on Privacy and Electronic Communications (ePrivacy Directive), 2002 O.J. (L 201) 37, https://perma.cc/YHA5-EFXV.

[11] Law No. 4624/2019, art. 21(1). The Greek limit is one year younger than the GDPR default of 16 years of age. The GDPR allows Member States to set a younger age of consent, provided that it is not below 13 years. GDPR art. 8(1).

[12] Law No. 4624/2019, art. 21(2).

[13] Id. art. 57(1) (implementing art. 12(1) of Directive 2016/680).

[14] An exception is Decision No. 112/2012 of the Greek Data Protection Authority, providing guidelines for the use of geolocation services for the tracking of vulnerable individuals and minors, available at https://perma.cc/RTS5-V2ND (in Greek). See Vassilios Kourtis, *Data Protection in the Internet: Greece*, in D. Moura Vicente, S. de Vasconcelos Casimiro (eds.), *Data Protection in the Internet* (2020), 220.

teachers or other persons, or (d) unreasonably show minors in dangerous situations.[15] Commercial communications for alcoholic beverages specifically directed to minors are also prohibited.[16]

Additionally, video-sharing platforms must take appropriate measures to protect minors from programs, user-generated videos and audiovisual commercial communications that may impair their physical, mental or moral development.[17] To protect minors, harmful content on video-sharing platforms such as gratuitous violence and pornography must be subject to strict access-control measures, such as age verification and parental control systems.[18] When video-sharing service providers obtain the personal data of minors through age-verification and parental control systems, it may not be processed for commercial purposes, such as direct marketing profiling and behavioral advertising.[19] Such providers are required to submit information related to the age-verification and parental control systems they implement to the National Broadcasting Council.[20] The law also "encourages" video-sharing service providers to take measures to prevent minors from excessive consumption of food and beverages that are not appropriate for them through the adoption of industry codes of conduct or general terms and conditions preventing the presentation of such foods and beverages.[21]

Law No. 2863/2000 mandates actors in the advertising industry to jointly adopt a code of conduct governing commercial communications in electronic media.[22] The self-regulation organization of the Greek advertising industry—the Greek Advertising Self-Regulation Council (Συμβούλιο Ελέγχου Επικοινωνίας (ΣΕΕ) [SEE])—administers the Greek Code of Advertising-Communications (Ελληνικου Κωδικα Διαφημισησ-Επικοινωνιασ (ΕΚΔ-Ε)[EKD-E](2007)).[23] The EKD-E is based on the International Chamber of Commerce's *ICC Advertising and Marketing Communications Code*,[24] and includes various rules and principles regarding the appropriate form and content of commercial communications directed to minors.[25]

---

[15] Law No. 4779/2021 (E.K.E.D. 2021, A:27), art. 14(5) (transposing art. 9 of Directive (EU) 2010/13), https://perma.cc/42VN-2TUK.

[16] Id. art. 14(4).

[17] Id. art. 32(1)(a).

[18] Id. arts. 32(6) and 9(1).

[19] Id. art. 32(7).

[20] Id. art. 32(6)(f),(h) and (10)(e).

[21] Id. art. 32(4).

[22] Εθνικό Συμβούλιο Ραδιοτηλεόρασης και άλλες αρχές και όργανα του τομέα παροχής ραδιοτηλεοπτικών υπηρεσιών [(Law on) the National Broadcasting Council and other authorities and bodies in the field of broadcasting], Law No. 2863/2000 (E.K.E.D. 2000, A:262), art. 9(1), https://perma.cc/J7NX-7UMM.

[23] EKD-E is available at https://perma.cc/9PZL-MF5S (in Greek).

[24] The 2018 edition of the ICC Code is available at https://perma.cc/R2Y2-F7XH.

[25] E.g. EKD-E, arts. 18, D7, and Annex II. The EKD-E, like the ICC Code on which it is based, differentiates between children (aged under 14 years) and teenagers (14-18), and includes more protective rules for the former class.

IV. Future Plans to Protect Children Online

Currently there appears to be no significant future plans or legislative efforts reported in public sources regarding rulemaking in the matter of the protection of personal data of minors.

Portugal

Eduardo Soares
Senior Foreign Law Specialist

SUMMARY The protection of children's personal data in Portugal relies on the European Union's General Data Protection Regulation, which was implemented in the country's domestic legislation in 2019. Portugal has yet to enact specific regulations to control the type of advertising that can be shown on platforms designed for children. However, the Advertising Code of 1990 regulates advertisements involving or designed for children.

I. Introduction

To implement the European Union's General Data Protection Regulation (GDPR)[1] into its domestic legislation, Portugal enacted Law No. 58 of August 8, 2019.[2] Law No. 58 applies to the processing of personal data carried out in the national territory, regardless of the public or private nature of the controller or the subcontractor, even if it is carried out in compliance with legal obligations or in pursuit of missions of public interest, applying all the exclusions provided for in article 2 of the GDPR.[3] Under the GDPR, the processing of personal data must comply with the principles of lawfulness, fairness, and transparency; limitation of purpose; data minimization; accuracy; storage limitation; and integrity and confidentiality.[4]

Law No. 58 was approved on June 14, 2019, promulgated on July 26, 2019, published on the Official Gazette on August 8, 2019, and entered into force on the following day of its publication.[5]

II. Data Protection for Children

Law No. 58 of August 8, 2019, establishes that under the terms of article 8 of the GDPR, children's personal data can only be processed based on the consent provided for in article 6(1)(a) of the GDPR and related to the direct offer of information society services when they are 13 years old.[6] If the child is under the age of 13, treatment is only lawful if consent is given by the child's legal representatives, preferably using secure authentication means.[7]

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), 2016 O.J. (L 119) 1, https://perma.cc/4HPB-DXKW.

[2] Lei No. 58/2019, de 8 de Agosto, art. 1, https://perma.cc/6DCB-V76G.

[3] Id. art. 2(1).

[4] GDPR art. 5.

[5] Lei No. 58/2019, de 8 de Agosto, art. 68.

[6] Id. art. 16(1).

[7] Id. art. 16(2).

According to article 6(1)(a) of the GDPR, processing must be lawful only if and to the extent that the data subject has given consent to the processing of his or her personal data for one or more specific purposes.[8]

The conditions for consent are set forth in article 7 of the GDPR, which include:

> 1. Where processing is based on consent, the controller must be able to demonstrate that the data subject has consented to processing of his or her personal data.
>
> 2. If the data subject's consent is given in the context of a written declaration, which also concerns other matters, the request for consent must be presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of the GDPR must not be binding.
>
> 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent must not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed thereof. It must be as easy to withdraw as to give consent.
>
> 4. When assessing whether consent is freely given, utmost account must be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[9]

Article 8(1) of the GDPR sets the conditions applicable to child's consent in relation to information society services. Where article 6(1)(a) of the GDPR applies in relation to the offer of information society services directly to a child, the processing of the personal data of a child must be lawful where the child is at least 16 years old (or a lower consent age if opted for by a Member State, such as 13 in Portugal). Where the child is below the age of 16 years (below 13 in Portugal), such processing must be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child.[10] The controller must make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.[11] Article 8(1) of the GDPR does not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.[12]

Although article 40 of the GDPR encourages member states to draw codes of conduct intended to contribute to the proper application of the regulation, it seems that Portugal has yet to produce a specific code of practice on standards of age appropriate design of relevant information society services likely to be accessed by children.[13]

---

[8] GDPR art. 6(1)(a).

[9] Id. art. 7.

[10] Id. art. 8(1).

[11] Id. art. 8(2).

[12] Id. art. 8(3).

[13] Id. art. 40.

III. Advertisements on Platforms Designed for Children

On October 23, 1990, Decree-Law No. 330 approved the Advertising Code, which applies to any form of advertising, regardless of the medium used for its dissemination.[14] According to article 3(1) of the Code, advertising is broadly defined as any form of communication made by entities of a public or private nature, within the scope of a commercial, industrial, artisanal or liberal professional activity, with the direct or indirect purpose of promoting the sale or alienation of any goods or services, or the promotion of ideas, principles, initiatives or institutions.[15]

Advertising especially directed at minors must always take into account their psychological vulnerability, abstaining, from:

> a) Directly inciting minors, exploiting their inexperience or credulity, to purchase a certain good or service;
>
> b) Directly encouraging minors to persuade their parents or third parties to buy the products or services in question;
>
> c) Containing elements liable to endanger their physical or moral integrity, as well as their health or safety, namely through pornography scenes or inciting violence;
>
> d) Exploiting the special trust that minors place in their parents, guardians or teachers.[16]

Minors can only be major players in advertising messages in which there is a direct relationship between them and the product or service advertised.[17]

Advertising for alcoholic beverages is not allowed to specifically address minors or introduce them to the consumption of such drinks.[18]

Commercial communications and advertising of any events in which minors participate, namely sporting, cultural, recreational or other activities, must not display or implicitly or explicitly mention any brand of alcoholic beverages.[19] In the places where these events are held, alcoholic beverage brands cannot be displayed or in any way advertised.[20]

Advertising is prohibited for alcoholic beverages, tobacco, or any kind of pornographic material, in educational establishments, as well as in any publications, programs, or activities especially aimed at minors.[21]

---

[14] Código da Publicidade, Decreto-Lei No. 330/90, 23 de Outubro, art. 1, https://perma.cc/9T75-MDKP.

[15] Id. art. 3(1).

[16] Id. art. 14(1).

[17] Id. art. 14(2).

[18] Id. art. 17(1)(a).

[19] Id. art. 17(5).

[20] Id. art. 17(6).

[21] Id. art. 20.

Advertising on websites, social networks, or mobile apps for foods and beverages of high energy value or high salt, sugar, or fat content addressed to minors under 16 years of age are prohibited.[22]

Gambling and betting advertising must be carried out in a socially responsible manner, respecting, in particular, the protection of minors as well as other vulnerable and at-risk groups. It must not, for example, suggest it is easy to obtain a win, or encourage excessive gambling or betting.[23]

It is strictly prohibited to advertise games and bets that target or use minors in the message.[24] Advertising of games and betting within or near schools or other places for children under the age of six is expressly prohibited.[25] It is also strictly forbidden to advertise games and bets near schools or other places intended for minors.[26]

Violations of the Advertising Code may be remedied by fines or an order for precautionary measures to suspend, terminate or prohibit such advertising, regardless of fault or proof of loss.[27]

IV. Future Plans to Protect Children Online

Our research did not reveal any future plans in Portugal for further legislation or regulations to protect children's privacy online.

[22] Id. art. 20-A(3)(d).

[23] Id. art. 21(1).

[24] Id. art. 21(2).

[25] Id. art. 21(3).

[26] Id. art. 21(4).

[27] Id. art. 41(1).

Romania

Georgiana Grozescu
Legal Research Fellow

SUMMARY As a European Union Member State, the provisions of the General Data Protection Regulation (GDPR) apply directly to Romania. To comply with the regulation, the Romanian Government has amended more than 1,500 laws and regulations that could involve the processing of personal data. The GDPR's implementing legislation created the institutional framework for its application. The National Supervisory Authority for the Processing of Personal Data is designated as the national regulator tasked with monitoring compliance with the regulation and applying sanctions and corrective measures to public authorities or private data operators that violate its provisions.

In Romania, when "information society services" are offered directly to children, consent must be obtained from the holder of parental responsibility before processing the personal data of a child under 16 years of age. Data controllers must make reasonable efforts to verify that consent was given by the holder of parental responsibility, but Romania has not yet issued any national guidelines for the implementation of these provisions.

General legislation concerning advertising provides for restrictions and prohibitions on products that may be advertised to children, including alcohol, tobacco, drugs or pornography. Audiovisual commercial communications, regardless of the type and duration, must comply with the principles for minors' protection. Audiovisual programs that may seriously impair the physical, mental or moral development of minors can be aired only if a conditional access system restricts their viewing. The personal data of children may be processed on a large scale for advertising, marketing and publicity activities through automatic means of regular monitoring or recording of behavior, but the data controllers doing so must conduct a data protection impact assessment first.

I. Introduction

Because Romania is a European Union (EU) Member State, the provisions of the EU's General Data Protection Regulation (GDPR)[1] are directly applicable. Some provisions, however, require the adoption of measures of application by the Member States for their implementation.

To comply with the regulation, the Romanian Government has amended more than 1,500 laws and regulations that could involve the processing of personal data.[2] This report details only legislation that is most relevant for that purpose.

[1] General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1, https://perma.cc/7T85-89ZQ.

[2] See, e.g., Law no. 209/2019 concerning payment services, Law no. 95/2006 concerning health reform, Law no. 127/2019 concerning public pensions, and Law no. 211/2004 concerning crime victims.

Romania has passed Law no. 190/2018, which entered into force on July 31, 2018.[3]. It designates the National Supervisory Authority for the Processing of Personal Data (NSA)[4] as the national regulator tasked with monitoring compliance with the regulation and applying sanctions and corrective measures to public authorities or private data operators that violate its provisions.[5] It details the conditions for processing certain data (genetic data, biometric data, health data, national identification number, and personal data in the context of employment) and sets out reprimands and fines as sanctions for violation of the GDPR's provisions.[6]

Law No. 129/2018,[7] which entered into force on June 24, 2018,[8] integrates into the powers of the NSA those created by GDPR for national regulators and details the procedure for monitoring compliance, processing complaints, and sanctioning violations, as well as judicial remedies.[9] It repeals Law No. 677/2001 on the Protection of Individuals Regarding the Processing of Personal Data and the Free Movement of Such Data,[10] and it states that all references to Law no. 677/2001 must be construed as references to the GDPR and to the law for its implementation.[11]

---

[3] Legea nr. 190/2018 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor) [Law no. 190/2018 on Implementing Measures to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation)], M.Of. [Official Bulletin] pt. I, no. 651, July 26, 2018, https://perma.cc/XJ92-V68A. The law establishes the measures needed to implement, at the national level in particular, the provisions of articles 6(2), 9(4), 37-39, 42, 43, 83(7), 85, and 87-89 of the regulation.

[4] The authority had already been established in 2005.

[5] Law no.190/2018, arts. 13, 14.

[6] Id. arts. 12, 15.

[7] Legea nr. 129/2018 din 15 iunie 2018 pentru modificarea şi completarea Legii nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, precum şi pentru abrogarea Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date [Law No. 129 of the 15th of June 2018 on Amending and Supplementing Law no. 102/2005 on Organisation and Functioning of the National Supervisory Authority for Personal Data Processing, as well as on Repealing Law no. 677/2001 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data], art. VIII (1), M.Of. no. 503, June 19, 2018, https://perma.cc/5G3K-2NNY. The law creates the institutional framework necessary to apply in Romania provisions of articles 51-55, 57-59, 62, 68, 77, 79, 80, and 82-84 of Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC.

[8] Id. art. VIII(2).

[9] Id. art. I.11.

[10] Lege nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, M.Of. pt. I, no. 790, Dec. 12, 2001, https://perma.cc/9ZN5-D47F.

[11] Law nr. 129/2018, art. V.

The NSA subsequently passed Decision No. 174/2018.[12] Under article 35(1), (7) of the GDPR, when a type of processing, in particular one using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons, the data controller or operator must first carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.[13] The decision details a list of situations in which data controllers must carry out a data protection impact assessment, such as video surveillance and processing on a large scale of special categories of data.[14]

II. Data Protection for Children

Under Law 272/2004 on Protection and Promotion of the Rights of the Child,[15] children have the right to have their public image and personal, private, and family life protected.[16] Any action that may affect that right is prohibited.[17]

Under the GDPR, when "information society services" are offered directly to a child under 16 years of age, consent by the holder of parental responsibility is needed for data processing to be lawful.[18] Member States may lower the age to 13,[19] but Romania has not done so. According to the Civil Code, consent by the holder of parental responsibility (who may be a parent or guardian) is usually required for any contract involving a child under 18 years old.[20] However, under the code, any processing of personal data, by automated or manual means, must observe the GDPR.[21] Consequently, consent by the holder of parental responsibility is mandatory only for processing the personal data of children under 16.

Data controllers must make reasonable efforts to verify that consent was given by the holder of parental responsibility.[22] Because children are regarded as particularly vulnerable, any information or communication to a child has to be easily understandable in clear and plain

[12] Decizia nr. 174/2018 din 18 octombrie 2018 privind lista operațiunilor pentru care este obligatorie realizarea evaluării impactului asupra protecției datelor cu caracter personal [Decision No. 174/2018 on the List of Processing Operations that Are Subject to the Requirement for a Data Protection Impact Assessment], M.Of. pt. I, no. 919, Oct. 31, 2018, https://perma.cc/W22V-YCTG.

[13] Id. pmbl.

[14] Id. art. 1.

[15] Lege nr. 272/2004 privind protecția și promovarea drepturilor copilului [Law 272/2004 on Protection and Promotion of the Rights of the Child], M.Of. pt. I, no. 159, Mar. 5, 2014, https://perma.cc/89L8-YXE9.

[16] Id. art. 27(1).

[17] Id. art. 27(2).

[18] GDPR art. 8(1).

[19] Id.

[20] Legea nr. 287/2009 privind Codul Civil al României (Romanian Civil Code), (republished), arts. 38-43, M.Of. pt. I, n. 505, July 15, 2011, https://perma.cc/QG3A-QNZQ.

[21] Id. art. 77.

[22] GDPR art. 8(2).

language.[23] Romania has not yet issued any national guidelines for the implementation of these provisions. The NSA website contains a reference to the Guidelines 05/2020 on consent under Regulation 2016/679 issued by the European Data Protection Board.[24] Under these guidelines, what is reasonable, both in terms of verifying that a user is old enough to provide their own consent, and in terms of verifying that a person providing consent on behalf of a child is the holder of parental responsibility, may depend upon the risks inherent in the processing as well as the available technology.[25] In low-risk cases, verification of parental responsibility via email may be sufficient.[26] Conversely, in high-risk cases, it may be appropriate to ask for more proof, so that the controller is able to verify and retain the information under article 7(1) of the GDPR.[27] Trusted third-party verification services may offer solutions that minimize the amount of personal data the controller has to process itself.[28] The guidelines also offer some examples.[29]

Under Romanian law, data controllers who process the personal data of children on a large scale through automatic means of regular monitoring or recording of behavior, including for advertising, marketing and publicity activities, must perform and submit a data protection impact assessment.[30]

The GDPR calls on EU Member States and their supervisory authorities to encourage the drafting of codes of conduct for the proper application of the regulation.[31] According to the latest available data, the NSA has neither drafted nor approved such a code yet.[32]

The NSA is empowered to investigate violations of GDPR provisions of its own accord or upon a complaint by a person whose rights have been infringed.[33] If the NSA finds a violation, it may apply corrective measures such as compelling the data controller or processor to comply with the requests of the data subject for the exercise of the subject's rights or informing the data subject

[23] Id. art. 12(1), recital 58.

[24] European Data Protection Board, Guidelines 05/2020 on Consent Under Regulation 2016/679, May 4, 2020, https://perma.cc/B52J-RYDP.

[25] Id. at 28.

[26] Id.

[27] Id.

[28] Id.

[29] Id.

[30] Decision no. 174/2018 on the List of Processing Operations that Are Subject to the Requirement for a Data Protection Impact Assessment, art. 1(1)(d).

[31] GDPR, art. 40.

[32] In 2019, the NSA received for approval 11 draft codes of conduct issued by professional organizations concerning banking, insurance services, credit services, private pensions, bailiffs, notary publics and gambling. According to its Annual 2019 Report, NSA did not approve any codes, https://perma.cc/G6HH-7B33 (in Romanian).

[33] Legea nr. 102/2005 privind înfiinţarea, organizarea şi funcţionarea Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, ch. IV, M.Of. pt. I, no. 947, Nov. 9, 2018, https://perma.cc/MU2L-P7WT.

about a personal data breach,[34] rectifying or deleting personal data, restricting processing, or withdrawing certification.[35] The NSA may apply a warning, a reprimand, or a fine.[36] The application of the fine is made under the conditions of GDPR's article 83.[37] The NSA may order the publication by the data controller or processor or of any corrective measures applied, with the costs incurred by the controller or processor.[38] In case of noncompliance with the measures ordered, tacit or express refusal to provide all the information and documents requested during the investigation procedure, or refusal to submit to the investigation, the NSA may order, by decision, the application of a cumulative fine of up to 3,000 Lei (about US$738) for each day of delay, calculated from the date established by the decision.[39]

III. Advertisement on Platforms Designed for Children

Under Law 148/2000 on Advertising, publications that are mainly designed for children are not allowed to display ads for tobacco or alcohol products.[40] Advertising for alcohol or tobacco products is not allowed to target children or depict children using such products.[41] Products and services destined for children are not allowed to display advertising containing elements that may adversely affect children (physically, morally, intellectually or psychologically); indirectly encourages children to buy products or services, taking advantage of their lack of experience; adversely affects the relationship between children and their parents or teachers; or unreasonably depicts children in dangerous situations.[42] Advertising of drugs or related substances is generally prohibited.[43] Only medications that are available over the counter can be advertised.[44] Violation of these provisions is punishable by a fine.[45]

The Romanian Council for Advertising, a professional organization for self-regulation in advertising, has issued the Code of Practice in Commercial Communications. It states that internet websites dedicated to products or services that are not recommended to children under

[34] Id. art. 16.

[35] Id.

[36] Id. art. 15.

[37] Id.

[38] Id.

[39] Id. art. 18(2).

[40] Legea nr. 148/2000 privind publicitatea, art. 12, M.Of. pt. I, no. 359, Aug. 7, 2000, https://perma.cc/MUB6-WXXQ.

[41] Id. art. 13(1), (2).

[42] Id. art. 16.

[43] Id. art. 14.

[44] Id. art. 17.

[45] Id. art. 23.

a certain age must take measures to limit the access of underage children.[46] The code also contains rules concerning the advertising of toys, food, and beverages to children.

Traditional audiovisual media services are covered by the Audiovisual Code adopted by the National Audiovisual Council of Romania. Under this code, audiovisual media service providers must respect the principle of the best interest of the child.[47] Child have the right to the protection of their public image and their intimate, private, and family life.[48] Audiovisual commercial communications, regardless of type and duration, must comply with the principles for minors' protection.[49] Commercial communication of erotic phone calls as well as of products and services with a sexual purpose are forbidden.[50] Broadcasting any kind of commercial communication or promotional material for pornographic products is forbidden.[51]

Audiovisual programs that could seriously impair the physical, mental, or moral development of minors can be aired only if a conditional access system restricts their viewing.[52] If an appropriate conditional access device is lacking, such programs can only be broadcast during the time period allowed for such content according to its age classification.[53] During video-on-demand audiovisual media services, programs that might impair the physical, mental, or moral development of minors can be made available only on condition that access restriction measures are provided for by means of a parental control system, so that minors cannot normally see or hear such programs.[54] Broadcasters cannot air studio audiovisual programs or live programs where people smoke, drink alcoholic beverages, or behave in an obscene way during the time period between 6 a.m. and 8 p.m.[55] Programs are classified according to strict criteria.[56] Audiovisual programs providing gambling services must comply with minors' protection conditions.[57] Gambling cannot be included in programs addressed to children, and they cannot be encouraged to take part in gambling, either.[58]

---

[46] Code of Practice in Commercial Communication art. 23.7 (Romanian Council Advert. 2021), https://perma.cc/3MFK-7P72.

[47] Decizia nr. 220/2011 privind Codul de reglementare a conținutului audiovizual art. 2, M.Of., pt. I, no. 174, Mar. 11, 2011, https://perma.cc/W8PW-9SJT.

[48] Id. art. 3(1).

[49] Id. art. 93.

[50] Id. art. 96(1).

[51] Id. art. 96(3).

[52] Id. art. 12(1).

[53] Id, art. 12(2).

[54] Id. art. 13.

[55] Id. art. 15.

[56] Id. arts. 19-21.

[57] Id. art. 89(3).

[58] Id. art. 89(4).

The same rules apply to on-demand audiovisual media services, according to Decision No. 320/2012 Concerning On-Demand Audiovisual Services.[59] However, this decision does not apply to websites that allow video sharing by individual private users, such as YouTube, Google, or Vimeo, or to internet search engines.[60]

The only restriction on processing the personal data of children is stipulated by Decision 174/2018. Data controllers that process the personal data of children on a large scale through automatic means of systematic monitoring or recording of behavior, including for advertising, marketing and publicity activities, must conduct a data protection impact assessment.[61] A data controller that does not observe these provisions is liable for a fine.[62] The NSA can apply corrective measures as well.

IV. Future Plans to Protect Children Online

No future plans to protect children's privacy online were identified.

[59] Decizia nr. 320/2012 privind furnizarea serviciilor media audiovizuale la cerere, M.Of. pt. I, no. 434, June 30, 2012, https://perma.cc/U53T-T6D6.

[60] Id. art. 2(3)(b), (f).

[61] Id. art. 1(d).

[62] GDPR, art. 83(4)(a); Law no. 190, art. 12.

Spain

Graciela Rodriguez-Ferrand
Senior Foreign Law Specialist

SUMMARY The Law on the Protection of Personal Data and Guarantee of Digital Rights implements the EU General Data Protection Regulation, providing the legal framework on data privacy protection. Data protection rights are exercised by parents or legal representatives of minors younger than 14 years of age, including the required consent for the processing of their personal data in cases required by law. Minors are also protected from inappropriate advertising online, with specific restrictions applicable to tobacco products and gambling. The data protection agency provides guidelines for minors, parents, and teachers on best practices to prevent breaches of privacy and exposure to inappropriate content.

I. Introduction

In Spain, the EU General Data Protection Regulation (GDPR)[1] and Organic Law 3/2018 of December 5, 2018, on the Protection of Personal Data and Guarantee of Digital Rights (Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales; LPDP)[2] constitute the legal framework applicable on privacy and data protection.

In implementing the GDPR, the LPDP aims at protecting the intimacy, privacy, and integrity of the individual, in compliance with article 18.4 of the Spanish Constitution, which provides that, to guarantee the honor and personal and family privacy of citizens and the full exercise of their rights, the use of information technology will be limited by law.[3]

The Agencia Espanola de Protección de Datos (AEPD) is the enforcement authority in charge of the protection of personal data in Spain.[4]

The LPDP applies to personal data as defined in the GDPR, being any information in text, image, or audio form that allows the identification of a person.[5] It regulates the obligations of the individual in any data transfer process to guarantee the security of the exchange.[6] Some data is

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR), 2016 O.J. (L119), https://perma.cc/VX6F-5JTL.

[2] Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LPDP), Boletin Oficial del Estado (B.O.E.) Dec. 6, 2018, https://perma.cc/7P49-UFAK.

[3] Id. art. 1; Constitución Espanola (CE) BOE Dec. 29, 1978, art. 18.4, https://perma.cc/N4WK-4D9U.

[4] LPDP art. 44.

[5] GDPR art. 4; LPDP art. 2.

[6] Id. art. 12.

considered to be of low risk, such as a person's name or email address, while other data is considered of higher risk because of its sensitive character, such as data related to a person's religion or personal health.[7] The processing of sensitive data requires the free, informed, specific, and unequivocal consent of the affected person.[8] Furthermore, the processing of personal data must be limited to that which is necessary for its intended purpose.[9]

The LPDP also provides for the protection of personal data on the internet.[10] In this regard, it implements the right to be forgotten and the right of portability, as well as mandating that consent be obtained in order to collect and use personal information.[11]

The LPDP also requires that the AEPD be notified of security breaches affecting protected personal data within a maximum period of 72 hours.[12]

According to the GDPR and the LPDP, the processing of personal data must be based on the principles of legality; trustworthiness; transparency; restrictive purpose in order to safeguard individual's vital and essential interests; accuracy; and data minimization.[13]

II. Data Protection for Children

Under the LPDP, minors and adults have the same personal data protection rights, as follows:

- Right of access, being the right to contact and obtain information from those responsible for the treatment of personal data regarding the way in which one's personal data is treated;
- Right to rectification, in order to have inaccurate personal data corrected;
- Right to be forgotten, being the right to request personal data be erased in specific circumstances, such as when it is no longer necessary, or if it was obtained without consent, etc.;
- Right to limitation of treatment, being the right to request the suspension of personal data treatment in certain situations, such as when the data processed is being challenged in terms of its accuracy or legality;
- Right of portability, requiring that, in case of automated treatment, personal data has to be structured in a format that allows it to be transferred to another data controller; and

[7] Id. art. 9.

[8] Id. art. 6.

[9] Id. art. 8.

[10] Id. arts. 70-86.

[11] Id. arts. 80-87 and 93.

[12] Id. art. 22.3.

[13] GDPR art. 5; LPDP arts. 4-10.

- Right to object to the treatment of personal data in certain situations, such as when the data is used for marketing purposes.[14]

Parents and legal representatives with parental authority over minors may exercise these rights on behalf of those under 14 years of age. Those older than 14 years of age may exercise the rights by themselves.[15] Therefore, minors 14 years of age or older may give consent for the processing of their personal data, unless a law specifically requires the consent of parents or guardians.[16] Minors younger than 14 years of age may only consent to the processing of their personal data upon their parent or guardian's consent.[17]

According to the LPDP, parents, guardians, or legal representatives "will ensure that minors make a balanced and responsible use of digital devices and the services of the information society in order to guarantee the adequate development of their personality and preserve their dignity and fundamental rights."[18]

Under the LPDP, the use or dissemination of images or personal information of minors in social networks, which may imply an illegitimate interference in their fundamental rights, will be subject to the intervention of the Public Prosecutor's Office, which will establish precautionary measures and protection provided for under the Organic Law 1/1996 on the Protection of Minors.[19]

The LPDP provides that the education system will guarantee the full insertion of students in the digital society. It will provide students with instruction to enable responsible consumption and critical and safe use of digital media, respecting and protecting personal data privacy.[20]

Educational institutions and any natural or legal persons that carry out activities in which minors participate are required to guarantee the protection of the best interests of the minor and their fundamental rights, especially the right to the protection of personal data, in the publication or dissemination of their personal information through information society services.[21]

The AEPD provides guidelines for parents, teachers, and children in order to protect them from breaches of privacy and exposure to inappropriate content on the internet.[22]

---

[14] LPDP arts. 12-18.

[15] Id.

[16] Id. art. 7.

[17] Id.

[18] Id. art. 84.1.

[19] Id. art. 84.2; Ley 1/1996 Orgánica de Protección del Menor, BOE Jan. 17, 1996, https://perma.cc/7LD6-2X7F.

[20] LPDP art. 83.1.

[21] Id. art. 92.

[22] AEPD, *Nota Técnica de Protección del Menor en Internet – Evita el Contenido Inapropiado Preservando su Privacidad* (Apr. 2020), https://perma.cc/G3NZ-FG2N.

In addition, the Law on Services of the Society of Information and Electronic Commerce provides that public administrations will promote voluntary codes of conduct, through coordination and consultation with corporations, associations, or commercial, professional, and consumer organizations.[23] These codes will take into account the protection of minors, establishment of common criteria agreed by the industry for the classification and labeling of content, and the adherence of the providers to them.[24] The codes of conduct must be accessible electronically and translated into other official languages of the European Union.[25]

The LPDP includes infractions that are designated as minor, serious, and very serious.[26] These are subject to monetary penalties, warnings, and disciplinary sanctions.[27]

III. Advertisements on Platforms Designed for Children

The General Law on Advertising provides that advertising aimed at minors that encourages them to buy a good or a service, exploiting their inexperience or ingenuity, or providing misleading or dangerous information regarding products and its safety, is illegal.[28]

The Law on Sanitary Measures against Smoking and Regulating the Sale, Supply, Consumption and Advertising of Tobacco Products prohibits any kind of advertising, promotion, or sponsorship of tobacco products in all media and supports, including vending machines and information society services, with limited exceptions.[29] One of the exceptions to the prohibition is publications that contain advertising of tobacco products that are edited or printed in countries that are not part of the European Union. However, this exception does not apply if the publication is primarily aimed at minors.[30]

The broadcast of programs or images in which the presenters, collaborators, or guests appear to be smoking, and the mentioning or display of brands, trade names, logos, or other identifying signs or associations with tobacco products is also prohibited in any media format, including information society services.[31]

---

[23] Ley 34/2002 de Servicios de la Sociedad de la Información y de Comercio Electrónico, BOE July 12, 2002, art. 18, https://perma.cc/4EGH-FMUA.

[24] Id.

[25] Id.

[26] LPDP arts. 70-74.

[27] *Cuales son las Sanciones por Incumplir el RGPD?*, Egida (Apr. 6, 2020), https://perma.cc/7CFP-ZSFL.

[28] Ley 34/1988, General de Publicidad, BOE Nov. 15, 1988, art. 3.b, https://perma.cc/VL7J-W79F.

[29] Ley 28/2005, de Medidas Sanitarias Frente al Tabaquismo y Reguladora de la Venta, el Suministro, el Consumo y la Publicidad de los Productos del Tabaco, BOE Dec. 27, 2005, art. 9.1.b, https://perma.cc/252A-2RGT.

[30] Id. art. 9.1.c.

[31] Id. art. 9.3.

Gambling operators may not direct advertising directly or indirectly to minors, or persuade or incite gambling to minors through advertising.[32] Commercial communications are specifically prohibited when they present gambling as a sign of maturity or indicative of the passage to adulthood, or where they are disseminated or placed in media, programs, applications, web pages, or digital content (specifically or together with links to web pages) aimed mainly at minors.[33] Commercial communications must include a warning that minors may not participate in gambling activities, such as "no minors," "18+," or similar.[34]

IV. Future Plans to Protect Children Online

The LPDP provided that, within one year of its entry into force, the government will draft a bill specifically aimed at guaranteeing the rights of minors in the face of the impact of the internet, in order to guarantee their safety and fight against discrimination and violence that is exerted on them through new technologies.[35] It appears that such a bill has not yet been submitted to the Congress.

[32] Real Decreto 958/2020, de Comunicaciones Comerciales de las Actividades de Juego, BOE Nov. 4, 2020, art. 11.1, https://perma.cc/ULP4-K9HJ.

[33] Id. art. 11.2.

[34] Id. art. 11.3.

[35] LPDP, Dispocisión Adicional Diecinueve.

Sweden

Elin Hofverberg
Foreign Law Specialist

SUMMARY The right to privacy and the protection against unlawful processing of personal data are protected in Sweden. As Sweden is a member of the European Union, the General Data Protection Regulation (GDPR) applies directly. The legal age to consent to the processing of personal information in Sweden is 13 years.

The Swedish Authority for Privacy Protection oversees compliance with the GDPR. It fined the City of Stockholm School Board for violating the GDPR when it stored student personal data in its digital attendance system.

Sweden prohibits the direct targeting of children in advertising, specifically prohibiting games from using advertisements aimed at children and requiring strict age requirements for games with adult advertising. The self-regulatory Swedish Advertising Ombudsman monitors compliance with advertising standards.

There are currently no bills pending in parliament concerning the protection of children's data online. A motion to increase fines for GDPR violations has been presented to the Constitutional Committee for further review.

I. Introduction

The right to privacy and the right to be protected against the unlawful compilation of personal data are protected in the Swedish Constitution.[1] The right to protection of one's personal data is established by European Union (EU) law in the General Data Protection Regulation (GDPR).[2] Although the GDPR is directly applicable in Sweden as of May 25, 2018, when the regulation entered into force, the GDPR has been codified in Swedish law through the Law on Additional Provisions to the EU Data Protection Regulation,[3] and the Regulation on Additional Rules to the EU Data Protection Regulation.[4] The law and regulation do not extend the protections otherwise found in the GDPR.

[1] 2 kap. 6 § 2st Regeringsformen (RF) (SF 1974:152), https://perma.cc/3DU4-FBWQ.

[2] General Data Protection Regulation (GDPR), 2016 O.J. (L 119) 1, https://perma.cc/JG59-NUXN.

[3] Lag med kompletterande bestämmelser till EU:s dataskyddsförordning (SFS 2018:218), https://perma.cc/MB2K-7KDT. Prop. 2017/18:, https://perma.cc/R2GW-GYCZ. SOU 2017:39, Ny dataskyddslag Kompletterande bestämmelser till EU:s dataskyddsförordning, https://perma.cc/T84S-868Y.

[4] Förordning med kompletterande bestämmelser till EU:s dataskyddsförordning (SFS 2018:219), https://perma.cc/CA75-FXLH.

Sweden has also implemented the EU e-Privacy Directive[5] in the Act on Electronic Communications, which among other things restricts the use of location data, and regulates when user consent is required for the collection or storage of data.[6]

The Swedish Authority for Privacy Protection (formerly the Swedish Data Protection Authority) is responsible for enforcing the GDPR.[7] Under the GDPR, the maximum monetary sanction that may be issued for not complying with an order from the Authority following a GDPR violation 4% of worldwide revenue.[8] Sweden has capped certain violations at SEK 5 million (about US$600,000) (for violations of article 83.4) and SEK 10 million (about US$1.2million) (for violations of articles 83.5 and 83.6).[9] Sweden follows the EU's guidelines for administrative fines under the GDPR.[10]

II. Data Protection for Children

In accordance with Swedish law and the GDPR, children aged 13 and up can provide consent to allow data processing.[11] Processing of data on children not yet 13 years old requires the consent of their legal guardian.[12]

In 2020, the Swedish Authority for Privacy Protection fined the City of Stockholm's Board of Education SEK 4 million (about US$476,000) for violating the GDPR when processing and storing personal data of underaged students.[13]

Several agencies have also issued guidance pertaining to children's use of the internet and social media. For example, the Child Ombudsman, the Swedish Authority for Privacy Protection, and the State Media Council have together issued a guide titled "Children and Youths' Rights on Digital Platforms."[14] The guide, which targets platform providers, recommends among other things that nudge techniques (design features to influence user behavior) not be used except to

[5] Consolidated Version of the Directive on Privacy and Electronic Communications (ePrivacy Directive), 2002 O.J. (L 201) 37, https://perma.cc/YHA5-EFXV.

[6] Lag om elektronisk kommunikation (LEK) (SFS 2003:389), https://perma.cc/3H9W-88VW.

[7] 3 § Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning; 6 kap. Lag med kompletterande bestämmelser till EU:s dataskyddsförordning. Currently the agency is called Integritetsskyddsmyndigheten (IMY) (Swedish Authority for Privacy Protection), formerly known as Datainspektektionen (Swedish Data Protection Authority).

[8] GDPR art. 83.6.

[9] 6 kap. 2 § Lag med kompletterande bestämmelser till EU:s dataskyddsförordning.

[10] Article 29 Data Protection Working Party, *Guidelines on the Application and Setting of Administrative Fines for the Purposes of the Regulation 2016/679* (Oct. 3, 2017), https://perma.cc/E92X-JMJ6.

[11] 2 kap. 4 § Lag med kompletterande bestämmelser till EU:s dataskyddsförordning.

[12] Id.

[13] *Serious Deficiencies in the Stockholm Online School Platform*, IMY (Nov. 24, 2020), https://perma.cc/UW6T-BRF2. Case available in Swedish at Datainspektionen, Diarienr. DI-2019-7024, https://perma.cc/6JYA-DSST.

[14] Barnombudsmannen, *Datainspektionen, Statens medieråd, Barns och Ungas Rättigheter på Digitala Plattformar* (2020), https://perma.cc/58HL-62YT.

promote the highest protection for personal data available, and that websites design their age verification methods to prevent children from providing an incorrect older age.[15] The guide is expressly inspired by the United Kingdom Information Commissioner's Office's code, *Age Appropriate Design: A Code of Practice for Online Services*, but does not have legal status.[16]

In addition, the State Media Council has published guidance on how parents can protect their children's personal data online.[17] It recommends that parents should:

- Talk to their child about privacy and content online.
- Think about what pictures [they] share of [their] children.

With the help of technology, it is possible to strengthen the protection of one's privacy in several different ways:

- In smartphones, it is possible to review what so-called rights different apps have and turn off access to, for example, address book or location positioning.
- On social media, it is often possible to decide what contacts that may see what you upload, or at least the opportunity to choose between making your account public or private.
- By choosing secure passwords and keeping your login details to yourself, you reduce the risk of hacked accounts. (See the text on why passwords are important.)
- By screenshot images and messages sent and shared online, it is possible to gather evidence of violations and threats, prior to a possible report to the company providing the service or to the police.
- Report any privacy breaches that you perceive as criminal to the police.[18]

III. Advertisements on Platforms Designed for Children

Under Swedish law, all advertisements must comply with good practice and custom.[19] In practice, this means that all advertisements that target children are prohibited. For example, advertisements targeting children expressly may not be part of games, including online games.[20] In addition, the International Chamber of Commerce Code on Advertisement and Communication restricts all advertisements that target children.[21] Game providers must also clearly state age requirements.[22]

[15] Id. at 43.

[16] Id. at 9. For more on the UK code, see the UK country survey in this report.

[17] *Hur Skyddar Jag Mitt Barns Digitala Integritet?,* Statens Medieråd, https://perma.cc/PZ2S-HFEK.

[18] Id.

[19] 5 § Marknadsföringslag (SFS 2008:486), https://perma.cc/H5R7-EEB2.

[20] 15 kap. 1 § Spellagen (SFS 2018:1138), https://perma.cc/6PHC-6FA6.

[21] ICC:s regler for marknadsföring och kommukation, https://perma.cc/A7KT-WAWU.

[22] 14 kap. 3 § Spellagen.

In addition, the Swedish Consumer Agency (Konsumentverket) has issued guidance for advertisements on blogs and in social media.[23] The guidance states that it must be clear when content is an advertisement, and that advertisements may never directly encourage children to purchase a product.[24] IAB Sweden, the national affiliate of the industry organization the Interactive Advertising Bureau, has issued specific industry guidelines for different use of advertisements, including for online influencers,[25] gaming,[26] and online video.[27]

Violations against advertisement law and custom is enforced by the Swedish Advertising Ombudsman (Reklamombudsmannen).[28] Rekalmombudsmannen is an industry self-regulation enforcement body that facilitates compliance by Swedish companies with meeting industry guidelines on advertisements.[29] Reklamombudsmannen is part of the EU network European Advertising Standards Alliance (EASA).[30] In 2018, Reklamombudsmannens opinionsnämnd found that an advertisement for educational services by the company Albert in Snapchat violated the ICC rules for advertisements, as it directly encouraged children to convince their parents to sign up for the service.[31]

IV. Future Plans to Protect Children Online

There are currently no bills pending in parliament regarding children's privacy online.

The Liberals (Liberalerna), which holds 19 out of 169 seats in parliament, have submitted a motion that Sweden increase the monetary fine for violations against data protection rules.[32] The motion has been assigned to the Constitutional Committee (Konstitutionsutskottet) for review and is not expected to be voted on in the near future.

[23] Konsumentverket, *Vägledning Marknadsföring i Sociala Medier*, https://perma.cc/G85N-GMB5.

[24] Id. at 4-5.

[25] IAB Sweden, *Standards & Guidelines Influencer Marketing* (Jan. 31, 2019), https://perma.cc/7G28-GCYL.

[26] IAB Sweden, *Gaming, Gamers & Esport* (Feb. 5, 2021), https://perma.cc/HLT9-6UFC.

[27] IAB Sweden, *Standards & Guidelines Online Video* (June 19, 2019), https://perma.cc/SNQ4-EQ73.

[28] *Vanliga frågor*, Reklamombudsmannen, https://perma.cc/NS4R-EEAQ.

[29] *Vanliga frågor*, Reklamombudsmannen, https://perma.cc/NS4R-EEAQ.

[30] *Homepage*, The European Advertising Standards Alliance (EASA), https://perma.cc/K2MK-DFHU.

[31] Rekalmomubdsmannens opinionsnämnd, Beslut Ärende 1801-12, May 16, 2018, https://perma.cc/3Q2V-QC9K.

[32] Motion 2020/21:1520, Skydda människors privatliv vid datainsamling, av Helena Gellerman och Robert Hannah (båda L), https://perma.cc/BPK7-SHGX.

United Kingdom

Clare Feikert-Ahalt
Senior Foreign Law Specialist

SUMMARY The UK has taken measures to provide children with special protections over the collection and use of their personal data they generate online. In September 2020, pursuant to a mandate in the Data Protection Act 2018, the Information Minister introduced a Code of Practice, titled the *Age Appropriate Design: A Code of Practice for Online Services*. The Code is comprised of 15 design standards for online services with special safeguards to protect children. The Code notes the difficulties of parents in exercising control over the use of their children's personal data, and places responsibility on Information Society Services (ISSs) to ensure age-appropriate use of personal data, respecting children's rights, and making decisions in children's best interests.

The Code has a 12-month transition period, providing service providers whose online sites or services include child users with time to redesign their webpages. The Information Commissioner's Office will oversee the implementation of the Code and has the power to take action to ensure it is complied with, including levying significant fines.

The UK has also implemented additional requirements for marketers utilizing online advertisements to ensure children are protected from those that are not age appropriate. An advertising code requires marketers to take care over the placement and content of any ads. Online behavioral advertisements are regulated by several overlapping laws, including the General Data Protection Regulation, the Privacy and Electronic Communications Regulations, the Committee of Advertising Practice Code, and the Age-Appropriate Design Code.

I. Introduction

The UK incorporated the European Union's General Data Protection Regulation (GDPR)[1] into its national law through the Data Protection Act 2018 (the DPA) on May 23, 2018.[2] The DPA regulates how personal information may be processed, "requiring personal data to be processed lawfully and fairly, on the basis of the data subject's consent or another specified basis."[3] There are six lawful bases for processing personal data: where an individual has given valid consent to data processing for a specific purpose; if the processing is necessary for contractual purposes; to enable

[1] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, https://perma.cc/CQ9F-AYNN. When the UK left the EU, it incorporated all EU law as it existed on December 31, 2020, into a new body of domestic law known as "retained EU legislation." References to the GDPR throughout this report refer to the Regulations incorporated in the domestic law of the UK.

[2] Data Protection Act 2018, c. 12, https://perma.cc/39Y3-H34A.

[3] Id. § 2(1)(a).

compliance with a legal obligation; if it is necessary to protect someone's life; to perform a task in the public interest; or if the processing is necessary for the official functions of the processor and there is not a good, overriding reason to protect the personal data.[4]

The DPA requires that any data collected should be limited in scope, necessary for the reasons it is processed, accurate, and kept up to date. It also requires providers of online services, which it calls Internet Society Services (ISSs), to adopt a risk-based approach when "using people's data, based on certain key principles, rights and obligations."[5]

Any personal data collected must be stored in a manner that enables the identification of the data subject and held for no longer than necessary. Personal data must be processed in a way that ensures the security of the data and protects against unauthorized processing, accidental loss, destruction, or damage. The DPA places a duty on the data controller to ensure the principles of the DPA are complied with, and to demonstrate how this compliance is achieved.[6] It also provides for regulatory oversight of its provisions and enforcement mechanisms to ensure it is implemented properly.

The GDPR requires Member States to protect children's data and must take extra care to ensure their interests are protected.[7] Recital 38 of the GDPR provides:

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.[8]

The DPA requires the Information Commissioner's Office (ICO), the independent body set up to uphold information rights,[9] to publish four Codes to supplement the implementation of the GDPR: a children's code, a data-sharing code, a direct marketing code and a data protection and journalism code.[10] This report provides an overview of the recently introduced Children's Code, titled the *Age Appropriate Design: A Code of Practice for Online Services* (the Code).[11]

---

[4] Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services* Annex C (ver. 2.1.114, Sept. 2, 2020), https://perma.cc/376E-YMNX.

[5] Id. at 10.

[6] Data Protection Act 2018, pt. 2, ch. 2.

[7] GDPR art. 8.

[8] Id. recital 38.

[9] *Who We Are*, ICO, https://ico.org.uk/about-the-ico/.

[10] Data Protection Act 2018 §§ 121-124.

[11] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4.

The DPA defines age-appropriate design as "the design of services so that they are appropriate for use by, and meet the development needs of, children."[12] The Code is comprised of 15 design standards, the first of which is to make the best interests of children a primary consideration.[13] While acknowledging that parents form a key role in protecting children, it notes the difficulties faced by parents in making informed choices or exercising control over how Information Society Services (ISSs) use children's data. The Code places responsibility on the ISS to "take responsibility for ensuring that the way their services use personal data is appropriate to the child's age, takes account of their best interests, and respects their rights; as well as supporting parents or older children in making choices (where appropriate) in the child's best interests."[14] This will require many ISSs to rework their sites to meet the standards in the Code; there will be "noticeable changes to the designs of websites that are accessed by children," with many ISSs having to put in substantial redesign work to comply with the Code.[15]

II. Data Protection for Children

The ICO estimates that one in five internet users in the UK is under the age of 18 and considers they are using an internet that is "not designed for them."[16] Section 123 of the DPA required the ICO to produce "a code of practice which contains such guidance as the Commissioner considers appropriate on standards of age-appropriate design of relevant information society services which are likely to be accessed by children."[17] Such services include not only those designed to be accessed by children, but also those where it is more probable than not a child will access it. This is a broad test, and the ICO notes:

> In practice, whether your service is likely to be accessed by children or not is likely to depend on: the nature and content of the service and whether that has particular appeal for children; and the way in which the service is accessed and any measures you put in place to prevent children gaining access.[18]

The ICO states that a common sense approach should be taken when determining these factors and recommends that ISSs that do not choose to implement the Code after determining their service is not likely to be accessed by children should clearly document the reasons for this decision.[19]

---

[12] Data Protection Act 2018 § 123.

[13] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 24.

[14] Id. at 10.

[15] Gareth Oldale, *5 Data Protection and Privacy Predictions for 2021*, Privacy & Data Protection 5 (Jan.-Feb. 2021) (available on Lexis-Nexis by subscription).

[16] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 3.

[17] Data Protection Act 2018 § 123.

[18] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 17.

[19] Id.

In drafting the Code, the ICO was required to consider that children have different needs at different ages,[20] along with the UK's obligations under the United Nations Convention on the Rights of the Child (UNCRC):[21]

> In particular, this code aims to ensure that online services use children's data in ways that support the rights of the child to: freedom of expression; freedom of thought, conscience and religion; freedom of association; privacy; access information from the media (with appropriate protection from information and material injurious to their well-being); play and engage in recreational activities appropriate to their age; and protection from economic, sexual or other forms of exploitation.[22]

The Code applies to online services based in the UK, or those based outside the UK that have a branch, office or other establishment that processes personal data in the course of activities in the UK. The Code also applies to an ISS that is based outside the UK if it offers services to users in the UK or monitors the behavior of users in the UK.[23]

A. Age Appropriate Design Code

The Code entered into force on September 2, 2020, and has a 12 month transition period, which is the maximum time allowed under the DPA.[24] The term ISS is defined broadly to include most online services.[25] ISSs will be required to comply with the provisions of the Code on September 2, 2021.[26] The Code is a statutory code of practice and the courts and tribunals must take its provisions into account when it is relevant in any proceedings before them.

The Code sets out 15 cumulative, interlinked standards of design, detailing how the principles, rights and obligations provided for in the DPA apply to children. "Child" is defined as anyone under 18 years of age.[27] Its coverage includes the use of inferred data, which is information inferred from online behavior or inferred from other information, and data collected directly from children.[28]

---

[20] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, Annex B.

[21] Data Protection Act 2018 § 123(4). See also ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 6.

[22] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 10.

[23] Id. at 18.

[24] Department for Digital, Culture, Media & Sport, *Explanatory Memorandum to the Age Appropriate Design Code 2020*, at ¶ 7.6 (June 2020), https://perma.cc/CD4K-XQ86.

[25] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 15-16.

[26] Id. at 9.

[27] Id. at 91.

[28] Id. at 11.

The Code aims

> to support compliance with the DPA and general principles of the General Data Protection Regulation ("the GDPR") to ensure online services appropriately safeguard children's personal data. The Code supports compliance with those general principles by setting out specific protections services need to build in when designing online services likely to be accessed by children. In particular, the Code sets out practical measures and safeguards to ensure processing under the GDPR can be considered 'fair' in the context of online risks to children.[29]

The Code is

> not intended as technical standards, but as a set of technology-neutral design principles and practical privacy features. The focus is on providing [benchmark] default settings which ensure that children have the best possible access to online services whilst minimising data collection and use, by default.[30]

Instead, the Code:

> sets out practical measures and safeguards to ensure processing under the GDPR can be considered 'fair' in the context of online risks to children, and will help you comply with [Articles 5, 6, 12-20, 22, 25 and 35].[31]

The Code aim to help organizations providing online services to children by "translat[ing] the GDPR requirements into design standards for online services, and tak[ing] into account the UNCRC that recognises the special safeguards children need in all aspects of their life."[32]

To meet the Code, ISSs must design their services in a way that complies with the GDPR, which makes it clear that children's personal data requires specific protections, as children are likely to have a lower level of understanding of the risks of the processing of their data."[33] The Code incorporates a key principle from article 3 of the UNCRC, that the best interests of the child shall be a primary consideration in actions concerning them. This principle should be specifically considered by ISSs when they design online services.[34]

B. Definition of Relevant ISS

As noted above, the Code applies to ISSs that "provide online products or services . . . that process personal data and are likely to be accessed by children in the UK. It is not only for services aimed

[29] *Explanatory Memorandum to the Age Appropriate Design Code 2020*, supra note 24, ¶ 7.1.

[30] Id. ¶ 7.2.

[31] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 11.

[32] *The Information Commissioner's Office (ICO) Age Appropriate Design Code*, Gov.uk (Feb. 10, 2021), https://perma.cc/74JQ-YN6G.

[33] Oldale, supra note 15.

[34] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 24.

at children."[35] "Relevant ISS" is defined in the Code as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."[36] The definition is broad and covers those that receive funding for the service, even if it not provided by the end user, such as through advertising. It encompasses search engines, social media platforms, online messaging services, content streaming services, news websites, retail websites, etc.[37]

The ICO has stated "[e]ssentially this [definition] means that most online services [are an] ISS."[38] Websites provided for preventative and health services, such as counselling or health screening, are exempt from the definition,[39] but general health, fitness and wellbeing services or apps are included. Websites provided by public authorities are not considered to be a relevant ISS as these types of services are typically not for commercial purposes. Websites that provide information about "real world" businesses, without allowing the purchase of goods or services online, also fall outside the scope of the Code.[40]

C. The 15 Standards

The 15 standards are considered to be flexible and do not ban or prescribe content. Instead, the standards aim for organizations to have an "age appropriate design reflecting a risk-based approach. The focus is on providing default settings which ensures that children have the best possible access to online services whilst minimising data collection and use, by default."[41] The 15 standards are described below.

1. Best Interests of the Child

Standard 1 provides that the best interests of the child should be a primary consideration in the design and development of online services that are likely to be accessed by a child.[42] This fulfils the obligation the ICO has to regard to the UNCRC when drafting the Code.[43] Notably the ICO provides the following instructions to ISSs:

> In particular you should consider how, in your use of personal data, you can:

---

[35] Id. at 9.

[36] Id. at 16.

[37] The ICO has provided a flow chart to help ISSs determine whether or not their sites fall within the Code, at id. Annex A.

[38] Id. at 16.

[39] Data Protection Act 2018 § 123(7).

[40] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 16.

[41] Id. at 5.

[42] Id. at 10. See also *Protecting Children's Digital Privacy with the Age Appropriate Design Code*, Children's Commissioner (Sept. 2, 2020), https://perma.cc/EU83-CTFH.

[43] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 24.

- keep [children] safe from exploitation risks, including the risks of commercial or sexual exploitation and sexual abuse;
- protect and support their health and wellbeing;
- protect and support their physical, psychological and emotional development;
- protect and support their need to develop their own views and identity;
- protect and support their right to freedom of association and play;
- support the needs of children with disabilities in line with your obligations under the relevant equality legislation for England, Scotland, Wales and Northern Ireland;
- recognise the role of parents in protecting and promoting the best interests of the child and support them in this task; and
- recognise the evolving capacity of the child to form their own view, and give due weight to that view.[44]

2. Data Protection Impact Assessments

ISSs must undertake a data protection impact assessment (DPIA) to "assess and mitigate risks to the rights and freedoms of children who are likely to access [the] service, which arise from your data processing."[45] When conducting the DPIA, the ISS must consider the different ages, capacities and developmental needs of child users. DPIAs have been described as "a key part of controller's accountability obligations and must be carried out before undertaking any processing that is likely to result in a high risk to the rights and freedoms of individuals."[46]

The ICO has stated that any processing conducted by online services will likely pose a high risk to children's rights and freedoms, and the DPIAs should specifically focus on these issues and assess and document the ISS's compliance with the Code. ISSs should regularly review DPIAs' and update them when necessary.

3. Age Appropriate Application

Standard 3 requires ISSs to take steps to establish the age of any users. It directs ISSs to use

> a risk-based approach to recognising the age of individual users and ensure you effectively apply the standards in this code to child users. Either establish age with a level of certainty that is appropriate to the risks to the rights and freedoms of children that arise from your data processing, or apply the standards in this code to all your users instead.[47]

The Code does not provide measures that ISSs should take to establish a user's age. It recommends that the method the ISS selects should "be appropriate to the risks . . . that arise from its data processing."[48] Methods that the ICO have suggested include:

---

[44] Id. at 25.

[45] Id. at 27. A template ISS can use to record DPIAs is contained in Annex D of the Code.

[46] Emma Erskine-Fox, *Understanding the ICO's Age Appropriate Design Code*, Privacy & Data Protection 4 (Apr.-May 2020) (available on LexisNexis by subscription).

[47] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 7.

[48] ICO, *ICO Answer to the Call for Submissions of the UNSRP* 8, https://perma.cc/EM5M-6T6S.

- a self-declaration in low-risk processing situations;
- the use of artificial intelligence to analyze how a user interacts with the webpage, although as this involves a level of data processing, this must comply with the requirements contained in the DPA;
- a third-party verification service; or
- by confirmation from existing account holders; or through other technical measures.[49]

The ICO advises that if an ISS cannot ascertain the age of the users of their service with any certainty on a level "that is appropriate to the risks to children arising from [its] data processing,"[50] the standards in the Code should be applied to all users. This ensures that any data obtained from children receive the correct processing protections.

4. Transparency

Standard 4 requires an ISS to be clear, honest and open about what users should expect when using its online services. It states that privacy information and other terms, policies and community standards provided to users "must be concise, prominent and in clear language suited to the age of the child."[51] It requires that in the event that a new use of personal data is activated, an additional, specific explanation known as a "just in time notice" should be provided to the user at that point in time. Depending upon the age of the child and the risks in processing, the notice should also direct them to speak with an adult and not proceed if they are unsure. In cases where the ISS wishes the notices to be "legally robust," explanations at the level appropriate for the correct age and developmental stage of the child user should be provided alongside more detailed information.

To help ensure transparency, information presented to child users should be done in a user-friendly manner and designed to appeal to the age of the child accessing the service, such as through cartoons, graphics, video and audio content, or other interactive content that attracts and interests the child user.[52] Full privacy information for parents should be provided alongside the information presented to children aged 12 and under.[53]

5. Detrimental Use of Data

Standard 5 notes that children's personal data should not be used "in ways that have been shown to be detrimental to their wellbeing, or that go against industry codes of practice, other regulatory provisions or Government advice."[54] To meet this standard, ISSs should ensure they are aware of, and in compliance with, any standards or codes of practice within their particular industries

[49] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 34.

[50] Id. at 35.

[51] Id. at 7.

[52] Id. at 19.

[53] Id.

[54] Id. at 7.

or sectors, along with government advice relating to the welfare of children regarding online or digital services.[55] In any case where the "use of personal data is clearly, or has been shown to be, detrimental to children's physical or mental wellbeing, this should be avoided."[56]

6. Policies and Community Standards

Standard 6 requires ISSs to not just state, but uphold and actively enforce, any published terms, policies and community standards.[57] For example, if personal data is collected from children to join or access services and the service does not do what claimed to do, the collection of personal data would be unlawful. In order to meet this standard, an ISS at a minimum should only use personal data collected in accordance with the privacy policy and uphold any policies or terms.[58]

7. Default settings

The ICO notes that children typically accept the default standards offered to them and rarely change them. Taking this into account, standard 7 requires ISSs to have the default setting as "high privacy." This requirement can be waived if the ISS can "demonstrate a compelling reason for a different default setting, taking account of the best interests of the child."[59] Thus, ISSs should only collect personal data required to provide each element of their online service and should not allow users' personal data to be visible to other users.[60]

8. Data Minimization

Standard 8 requires ISSs to collect only the minimum amount of personal data needed to deliver each individual element of the service when a child user is knowingly and actively using the service. Any data collected should be retained for the shortest amount of time required. Standard 8 notes that children should be provided with clear information and separate choices over each individual element of the service they wish to use. Personal data collected from children should not be "bundled," as doing so means the ISS is "effectively collecting personal data for different purposes."[61]

9. Data Sharing

Any personal data collected from children should not be disclosed or made visible to third parties unless there is a compelling reason for doing so and the best interests of the child have been considered. Standard 9 notes that any settings that permit general or unlimited sharing of a child's personal data will typically not be in compliance with the Code.

---

[55] Id. at 44.

[56] Erskine-Fox, supra note 46.

[57] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 47.

[58] Id.

[59] Id. at 61.

[60] Id.

[61] Id.

The standard provides several examples of compelling reasons to share data, including to prevent child sexual exploitation, or to prevent or detect crimes against children. It specifically states that selling personal data collected from children for commercial reuse "is unlikely to amount to a compelling reason for data sharing."[62]

ISSs should further refrain from sharing children's personal data if they can

> reasonably foresee that the sharing could result in third parties using personal data in a manner detrimental to the child. Providers should obtain assurances from any recipients about the use of personal data and should carry out due diligence on recipients' data protection practices. [63]

10. Geolocation

Standard 10 requires that geolocation capabilities, meaning the capability to obtain data that reveals the geographical location of a user's device, should be turned off by default. The standard notes the potential for abuse of such data and its significance in relation to the physical safety of children. It also notes the potential for use of such data to "fail to respect the child's rights under the UNCRC to privacy, freedom of association, and freedom from economic exploitation, irrespective of threats to their physical safety."[64]

In cases where there is a compelling reason for geolocation data to be turned on, an obvious sign must be provided to child user that such tracking is active and must be return to the default off setting at the end of each session. Any geolocation data that is processed also falls within the definition of location data within the Privacy and Electronic Communications Regulations (PECR),[65] and additional requirements must be met when processing such data.[66]

11. Parental Controls

Standard 11 requires ISSs that provide parental controls, which are tools that enable parents to limit or monitor their child's online activity or track their location, to make it clear to child users that such controls are in place and to notify them if they are being tracked or monitored.[67] The information provided should vary according to the child's age, for example for children under the age of nine, the information could take the form of a video or audio explaining what controls are in place and why.[68]

---

[62] Id.

[63] Erskine-Fox, supra note 46.

[64] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4.

[65] Privacy and Electronic Communications (EC Directive) Regulations 2003, SI 2003/2426, https://perma.cc/4PFG-FXVT.

[66] See also *Location Data*, ICO, https://perma.cc/RG3Q-XNJH.

[67] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 61.

[68] Id.

12. Profiling

Profiling is defined in the GDPR as

> any form of automated processing of personal data consisting of the use of personal data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour location or movements.[69]

Profiles are generated based on a user's online activity and are specifically mentioned in Recital 38 of the GDPR as an area in which children should receive specific protection. Standard 12 notes that, while profiling must be off by default, it is permissible to profile a user if consent has been obtained and privacy settings are in place.

Cookies are regulated by the PECR, which requires ISSs to inform users that cookies are being used, what they do, and why. ISSs must obtain a person's consent to store a cookie on their device.[70] The use of cookies also falls under this standard 12 if they are used for the purposes of profiling. Thus, the regulations contained in the PECR must be followed for the placement of cookies, and the GDPR and the code must be followed "for the underlying processing of personal data (profiling) that the cookie supports or enables."[71]

Profiling used for behavioral advertising to fund a service that is not part of the core service the child is accessing must have a privacy setting. In cases where cookies are essential to the provision of core services, the privacy setting will not be appropriate and, provided the ISS has a lawful basis for the profiling, consent will not be required for the cookie.[72] Cookies used to profile users in order to comply with the implied age verification requirements of the GDPR or to apply the standards of the Code are considered to be essential and, provided the information is only used for these purposes, no consent is required for the cookie.

Cookies that are not essential to the service the child is accessing, or for optional, non-core services, should be subject to a privacy setting that allows the child to control the processing of their personal data, and that provides a lawful basis for any processing connected with data provided by the cookie. In this situation, if there is a lawful basis for the underlying processing, consent for the use of the cookie is not required, "as the child is specifically requesting to access part of [the ISS's] service and the cookie is strictly necessary for this purpose."[73]

In cases where profiling is lawful, the ISS is responsible for implementing measures to ensure the profiling does not suggest content inappropriate to the child user. The standards note that the ISS

---

[69] GDPR art. 4(4).

[70] Privacy and Electronic Communications (EC Directive) Regulations 2003, reg. 6. See also *What are the Rules on Cookies and Similar Technologies?*, ICO, https://perma.cc/SPW5-ZXZL.

[71] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 66.

[72] Id.

[73] Id.

should test their algorithms to assess whether the methods implemented are effective.[74] The Code states:

> If you are using children's personal data to automatically recommend content to them based on their past usage/browsing history then you have a responsibility for the recommendations you make. This applies even if the content itself is user generated. In data protection terms, you have a greater responsibility in this situation than if the child were to pro-actively search out such content themselves. This is because it is your processing of the personal data that serves the content to the child. Data protection law doesn't make you responsible for third party content but it does make you responsible for the content you serve to children who use your service, based on your use of their personal data.
>
> Your general approach should be that if the content you promote or the behaviours your features encourage are obviously detrimental, or are recognised as harmful to the child, in one context (eg marketing rules, film classification, advice from official Government sources such as Chief Medical Officers' advice, PEGI ratings) then you should assume that the same type of content or behaviour is harmful in other contexts as well. Where evidence is inconclusive you should apply the same precautionary principle.[75]

13. Nudge Techniques

Standard 13 requires ISS providers to refrain from using nudge techniques—design features which lead or encourage users to follow the designer's preferred paths in the user's decision making—to:

- encourage children to provide personal data that is not necessary for the services they are using,
- obtain additional unnecessary personal data from children, or
- encourage them to turn off or otherwise weaken the default privacy protections.[76]

The Code notes that nudge techniques may be used for pro-privacy decisions, or to promote health and wellbeing.[77]

14. Connected Toys and Devices

Children's toys and devices that collect personal data and send it to a network connection—such as a fitness band, talking teddy bear or "hub" device—are of particular concern to the ICO. Standard 14 requires these devices to carry clear packaging and product leaflet or instructions that describes how personal data collected by the device is processed. This information should be made available to individuals prior to purchasing or setting up the device. The Code

[74] Id. at 69.

[75] Id.

[76] Id. at 72.

[77] Id.

recommends that should a "just in time" notice be warranted, it should be communicated using audio messages, or by only allowing the default settings to be changed through an app that provides more information.[78]

If the seller of the product uses a third party to connect the device to the internet, the third party's responsibilities depend upon whether they process the data on the seller's behalf, or if they are a data controller. The Code notes that sellers using a third party are still required to comply with the obligations contained in the GDPR as well as the Code, and must ensure that the third parties they use do so also.[79]

15. Online Tools

Standard 15 of the Code requires ISSs to "[p]rovide prominent and accessible tools to help children exercise their data protection rights and report concerns."[80] The rights relevant to this standard are contained in Articles 15-22 of the GDPR and include the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, and rights regarding automated decision making and profiling.[81]

Standard 15 requires tools to be prominently displayed, age appropriate, and easy to use. A mechanism should be in place to allow the child user to indicate whether the request or complaint is urgent and why, along with a method to prioritize such requests or complaints. When the user submits a request or complaint to the ISS, a mechanism for tracking the progress of any request or complaint should be provided, along with information about the timelines for responding to requests.[82]

D. Enforcement and Penalties

The ICO states in the Code that data protection relating to children is a one of its regulatory priorities[83] and that it

> consider[s] that the public interest in protecting children online is a significant factor weighing in the balance when considering the type of regulatory action. This means that where see harm or potential harm to children we will likely take more severe action against a company than would be the case for other types of personal data.[84]

[78] Id. at 78.

[79] Id.

[80] Id. at 80.

[81] *Guide to the General Data Protection Regulation (GDPR): Individual Rights*, ICO, https://perma.cc/8UC8-S6NX.

[82] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 83.

[83] Id. at 88.

[84] Id. at 90.

The Code is not legally binding; however, section 127 of the DPA requires the ICO to take the Code into account when determining if an ISS has complied with the data protection obligations contained in the GDPR or PECR.[85] The ICO has stated that how ISSs conform to the code will "be a key measure of [their] compliance with data protection laws."[86] The ICO has stated that while it will assess any conformity to the Code with the headline standards, the Code as a whole is provided to help ISSs understand how they can implement each standard properly.[87] The ICO will monitor compliance with the Code through a series of measures including using intelligence gathering, auditing and assessment powers, and reviewing complaints.[88] ICO has stated that it will encourage conformance with the standards and will "focus[] on organisations and individuals suspected of repeated or wilful misconduct or serious failure to comply with the law."[89] The ICO states:

> Where we find issues we take fair, proportionate and timely regulatory action with a view to guaranteeing that individuals' information rights are properly protected. We will take account of the size and resources of the organisation concerned, the availability of technological solutions in the marketplace and the risks to children that are inherent in the processing. We will take a proportionate and responsible approach, focusing on areas with the potential for most harm and selecting the most suitable regulatory tool.[90]

The Code notes that an ISS failing to comply with its provisions "may find it difficult to demonstrate compliance with the law and . . . may invite regulatory action."[91]

The ICO has a number of tools it can utilize to take action against organizations that fail to comply with the Code, such as issuing warnings, reprimands, stop now orders and fines of up to £17.5 million (approximately US$25 million), or 4% of a company's global turnover.[92] It has stated that the efforts an ISS has made to conform with the Code will be considered, and those that have clearly documented their approach will be more likely to be provided with time to comply. The ICO will be more likely to take formal action towards an ISS that has not taken steps to comply with the Code and has "evidence or constructive knowledge that children are likely to access [its] service[s], and clear evidence of significant risk arising from the use of children's data."[93]

[85] Data Protection Act 2018 § 127.

[86] Id. at 88.

[87] Id. at 13.

[88] Id. at 89.

[89] ICO, *Age Appropriate Design: A Code of Practice for Online Services*, supra note 4, at 89.

[90] Id.

[91] Id. at 11.

[92] Id.

[93] Id.

E. Review of the Code

The ICO must keep the Code under review. If it determines any amendments to the Code are necessary, it is under a duty to consult the Secretary of State and other appropriate parties. In addition to the duty to keep the Code under review, the ICO has stated it will review the Code a year after it comes into force to assess whether it is meeting its aims.[94]

F. Reaction to the Code

The ICO held a six-month consultation period to solicit public views on the Code.[95] Respondents to the consultation who had favorable views considered the Code was an opportunity to protect children's privacy and improve "expectations and norms for children online." Others expressed concern that the Code was too restrictive and would increase costs and discourage innovation, and that verifying the age of a child and obtaining parental consent would pose a challenge, especially in light of the international aspect of the internet.[96] Some ISS expressed concern

> that the Code could reach beyond the ICO's regulatory remit for data protection, and could result in regulatory overlap, duplication or potential inconsistency and could overburden services which are already heavily regulated.[97]

III. Advertisements on Platforms Designed for Children

A. Advertising Codes

In the UK, non-broadcast advertising is industry self-regulated by the Advertising Standards Authority (ASA), which enforces advertising codes.[98] The Committee of Advertising Practice (CAP) is responsible for publishing these codes.[99] In 2011, the role of the ASA was extended to "cover marketing communications on companies' own websites and in other third-party space under their control, such as on social networking sites."[100] This extension was done with the aim of protecting children, defined in the CAP Code as those under the age of 16 years old,[101] online.[102]

---

[94] *Explanatory Memorandum to the Age Appropriate Design Code 2020*, supra note 24, ¶ 13.

[95] ICO, *Consultation on Age Appropriate Design: A Code of Practice for Online Services* (2019), https://perma.cc/AX8J-X23H.

[96] *Explanatory Memorandum to the Age Appropriate Design Code 2020*, supra note 24, ¶ 9.

[97] Id. ¶ 9.8.

[98] House of Commons Library, *Advertising to Children* 7(Briefing Paper #8198, Mar. 2021), https://perma.cc/D6J8-WTWR.

[99] Id.

[100] Id. at 6.

[101] Committee of Advertising Practice, *The CAP Code* Rule 5 (12th ed.), https://perma.cc/XM4J-NTUB.

[102] House of Commons Library, *Advertising to Children*, supra note 98, at 19.

In 2017, additional guidance was provided to ensure that advertisements targeted at users under the age of 12 can be easily identified as such.[103]

The ASA "advise[s] marketers to check the audience profiles of any media they plan to advertise in, online and offline, in order to satisfy themselves that they are not at risk of targeting the wrong age groups."[104] The ASA has further stated:

> The [CAP] Code has an impact on where advertisements can be placed and the ASA has issued guidance on the placement of advertisements. There should be no ads that are age-restricted either in or around media that is obviously directed to the protected age category. This rule applied regardless of the method of targeting this ad. The rules have three key implications for different approaches to ad placement:
>
> - No age-restricted ads should appear in or around media obviously directed at the protected age category irrespective of the method of targeting.
> - Where marketing communications are directed at audiences based on data held by the marketer, media platform and/or other third party, targeting measures must be utilized to prevent the likelihood of those in the relevant protected age category from receiving them.
> - In one-to-many media [an area where the audience cannot be determined from a simple assessment], marketers must not place ads where children or children and young people are likely to make up more than 25% of the audience.

The CAP Code does not specify the type of data marketers should use to ascertain these percentages, but advises them to use data to show that over 75% of the audience is not within the protect age range.[105] The ASA has stated that it expects marketers to use all the tools available to them, including interest-based targeting and linked external data, to ensure that ads are targeted to age-appropriate users, noting that advertisers should factor in that children may misreport their age.[106]

In addition to general rules relating to advertisements, the CAP Code contains restrictions that specifically apply to children. Sexualized imagery of anyone who looks younger than 18 years of age is prohibited;[107] any advertisement that will result in a child's physical, mental or moral harm, such as frightening imagery that in a medium likely to be seen by children, is prohibited;[108] portraying children taking part in unsafe activities is prohibited; and advertisements for age restricted products, such as alcoholic drinks, gambling products, lotteries, electronic cigarettes and dieting products or services should not be displayed, or designed to appeal to, persons under

[103] Committee of Advertising Practice, *Recognition of Advertising: Online Marketing to Children Under 12: Advertising Guidance*, https://perma.cc/U35T-BL6Q.

[104] *Making Advertising to Children 'Child's Play'*, ASA (Nov. 26, 2020), https://perma.cc/5944-UF3P.

[105] CAP, *Media Placement Restrictions: Protecting Children and Young People: Advertising Guidance* 6, https://perma.cc/HVT9-KYNR.

[106] *Children: Targeting*, ASA (Aug. 1, 2018), https://perma.cc/T2MZ-Z9J4.

[107] Committee of Advertising Practice, *The CAP Code*, supra note 101, Rule 4.8.

[108] Id. Rule 5.1.

16 or under 18, depending upon the product.[109] CAP recently published additional guidance on age-restricted ads online that restrict children under the age of 16 years from being targeted with marketing communications for food or soft drinks that are high in fat, salt or sugar and from any that advertise the lottery.[110]

B. Behavioral Advertising

The ICO has stated that it acknowledges the importance of the revenue created by advertisements to the media industry and that the risks posed by behavioral advertising are lowered when advertisers apply the ASA codes.[111] The current law governing online behavioral advertising is contained in overlapping areas, including the GDPR, the PECR, the Code and the CAP Code. The ASA regulates online behavioral advertising; it requires businesses to disclose when they are collecting and using information for this purpose and to provide users the ability to opt out from providing information for this purpose. While the CAP Code regulates online behavioral advertising, it does not require user consent for businesses or organizations to place a cookie on a browser.[112] This area falls within the remit of the ICO and the laws contained in the GDPR and PECR, discussed in part II.C.12 above. For children, standard 12 of the Code, discussed above, further requires profiling to be turned off by default for child users, or if the age of the user cannot be established, turned off for all users.[113]

C. Enforcement

If the CAP Code is breached, the ASA has a number of tools at its disposal. It can issue an alert advising its members and media to withhold services, including access to advertising space; withdraw or withhold trading privileges, such as bulk mail discounts; requiring repeat or serious offenders to have their marketing reviewed prior to publication; and impose digital sanctions, such as the removal of a company's advertisements if it links to a page with non-compliant marketing materials.[114]

The tools available to the ICO for enforcement are detailed in part II.D above.

IV. Future Plans to Protect Children's Online Privacy

There is currently no additional legislation or policy that the government is considering to protect children's online privacy.

---

[109] Id. See also Committee of Advertising Practice, *Age-Restricted Ads Online: Advertising Guidance* 3, https://perma.cc/6QFL-YCT6.

[110] *Children: Targeting*, ASA, supra note 106.

[111] *Explanatory Memorandum to the Age Appropriate Design Code 2020*, supra note 24, ¶ 9.8.

[112] *What We Cover*, ASA, https://perma.cc/T2MZ-Z9J4.

[113] *Explanatory Memorandum to the Age Appropriate Design Code 2020*, supra note 24, ¶ 10.

[114] House of Commons Library, *Advertising to Children*, supra note 98, at 16.