Volume 1, Number 3 May–June 2024

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL

fastcase FULL COURT PRESS

The Global Regulatory Developments Journal

Volume 1, No. 3 May–June 2024

THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL (ISSN 2995-7486) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

The photo on this journal's cover is by Gaël Gaborel—A Picture of the Earth on a Wall—on Unsplash

Cite this publication as:

The Global Regulatory Developments Journal (Fastcase)

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE GLOBAL REGULATORY DEVELOPMENTS JOURNAL, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to international attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and others interested in global regulatory developments.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at morgan.wright@vlex.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2995-7486

European Digital Compliance: Key Digital Regulation and Compliance Developments

Alistair Maughan, Andreas Grünwald, Charlotte Walker-Osborn, Christoph Nüβing, and Sana Ashcroft*

In this article, the authors review some of the main digital regulatory and compliance developments that took place recently in the European Union. The authors also report on new rules relating to the repair of goods, greenwashing claims, online contract withdrawal rights, and auto-renewal subscriptions.

Organizations across Europe have numerous developments to stay on top of, with various digital compliance changes regularly being proposed, debated, and enacted by legislative and regulatory bodies across the region. This article reviews some of the main digital regulatory and compliance developments that took place in the final quarter of 2023, which was a busy few months for digital regulation in the European Union.

In addition to the heavily publicized EU Artificial Intelligence (AI) Act, the European Union has moved forward with regulations relating to child sexual abuse material, product liability laws affecting digital products and services, media freedom, the EU Data Act, and the EU Cyber Resilience Act. Not to be outdone, the United Kingdom enacted its controversial Online Safety Act. This article also reports on new rules relating to the repair of goods, greenwashing claims, online contract withdrawal rights, and auto-renewal subscriptions.

EU AI Act—Landmark Law on Artificial Intelligence Approved by the European Parliament

With extraterritorial reach and wide-reaching ramifications for providers, deployers, and users of artificial intelligence (AI), the Artificial Intelligence Act was approved by the European Parliament

The Global Regulatory Developments Journal / May–June 2024, Vol. 1, No. 3, pp. 151–175.

ISSN 2995-7486.

(EP) on March 13, 2024. The text of the approved version is based on the political agreement that the EP reached with the Council of the European Union in December 2023. The Act aims to safeguard the use of AI systems within the European Union as well as prohibiting certain AI outright.

The Act is subject to a final linguist check and will also need to be formally endorsed by the European Council. It is expected to be finally adopted around June 2024. It will enter into force 20 days after its publication in the *Official Journal of the European Union* and will be fully applicable 24 months later. However, certain provisions and obligations around prohibited AI practices and general purpose AI (GPAI) will come into force sooner.

Prohibited AI Practices

Certain AI practices that are deemed to pose an unacceptable risk to individuals' rights will be banned. The list of banned AI systems has been expanded in the final text to include practices such as untargeted scraping of facial images from closed-circuit television or the internet for facial recognition databases.

High-Risk AI Systems

The Act places several detailed obligations on what it categorizes as "high-risk AI." Examples of high-risk AI uses include use of AI systems in critical infrastructure, education and vocational training, employment, essential private and public services, certain systems in law enforcement, migration and border management, justice, and democratic processes like influencing elections. For high-risk AI systems, organizations must assess and reduce risks, maintain use logs, be transparent and accurate, and ensure human oversight.

Provisions Relating Specifically to General Purpose AI

The Act includes a two-tiered regime for providers of GPAI models that are trained with a large amount of data. Obligations on all GPAI providers obligations around transparency, creation of technical documentation and summaries of training data used. There are more stringent requirements that additionally apply to

GPAI that have systemic risk. GPAI systems can also qualify as high-risk AI systems if they can be used directly for at least one purpose that is classified as high risk.

Exemptions from the Act

The Act contains certain exceptions, for example, for certain free and open-source AI models as well as certain AI used for national security purposes.

Deepfakes and Chatbots

The Act requires that (save for certain public interest exemptions) artificial or manipulated images, audio, or video content (i.e., deepfakes) need to be clearly labeled as such. Similarly, when AI is used to interact with individuals (e.g., via a chatbot), it must be clear to the individual that they are communicating with an AI system.

Application of Copyright Law to AI Systems and Rights to Opt Out

The legal implications of intellectual property law in AI systems are a large topic. A key point in the Act to note is that, for use of copyrighted works for training purposes, GPAI providers must observe opt-outs made by rights holders, which will affect which data can be used for training purposes if an express opt-out has been delivered. The Act itself does not expressly deal with potential copyright issues relating to the output of the AI models. There are already several litigations regarding this area both in Europe and beyond. Over time, further legislation as well as the courts and private actors are likely to shape solutions both within the European Union and globally.

Enforcement and Increased Penalties

The maximum penalties for noncompliance with the Act were increased in the final draft. There are a range of penalties and fines depending on the level of noncompliance. At their highest level, an

organization can be fined an astounding €35 million or 7 percent of global annual turnover.

Interaction with Data Protection Laws

The final text clarifies that both individuals and supervisory authorities keep all their rights under existing EU data protection laws and that the Act does not affect the responsibilities of providers and deployers of AI as controllers or processors under the GDPR. The Act, however, has a far broader scope given it applies to all data.

Limited Rights for Individuals

The Act bestows rights on individuals to obtain an explanation of a decision made by a deployer of high-risk AI system based on the output from such high-risk AI system, where the decision has legal effects or similarly significantly affects that person and to complain to a supervisory authority if the individual considers that there is an infringement of the Act.

What's Next?

As mentioned above, the AI Act is expected to be formally endorsed by the Council before the end of the European Parliament's legislature in June 2024 and will then be subject to various transition periods as mentioned above. In the meantime, compliance efforts continue apace!

Regulation on Child Sexual Abuse Material: European Parliament Proposes More Limited Regulatory Obligations

In November 2023, the EP adopted its position[1] on a proposal on the so-called CSAM (Child Sexual Abuse Material) Regulation, which relates to child sexual abuse material. In a number of respects, the EP's approach is less onerous for digital service providers than the European Commission's original proposals.

The CSAM Regulation was first proposed by the Commission in May 2022. It aims to introduce a framework for providers of

certain digital services operating in the European Union to detect, report, and remove online child sexual abuse available via their services—including CSAM and child solicitation (so-called cyber grooming).

What's New?

The EP has suggested some key changes to the Commission proposal that would affect the impact of the CSAM Regulation on in-scope services. Most importantly:

- The EP suggests limiting the scope of risk management obligations in relation to online child sexual abuse. These obligations would only apply to (1) "very large online platforms" designated under the EU's Digital Services Act, and (2) services that are found to be substantially exposed to online child sexual abuse, video games with in-game communications features, porn websites, and services targeting children. The Commission proposal included no such limitation.
- The EP suggests that all services targeting children must adopt a suite of technical and organizational youth protection measures, including restrictive default settings, parental controls, and specific content moderation. If adopted, this would become the most broadly scoped and most comprehensive provision on youth protection obligations at the EU level.
- In relation to app stores, the EP suggests limiting the scope of specific risk management obligations to app stores provided by companies designated as "gatekeepers" under the EU's Digital Markets Act, while also severely limiting the burden associated with relevant substantive obligations.
- The EP also suggests severely limiting the scope of so-called detection orders—that is, orders to search users' content and communications for known or new CSAM. These orders would not lead to indiscriminate searches (as suggested by the Commission) but rather remain limited to "suspicious" accounts.
- The EP suggests limiting the scope of detection and removal orders in relation to cloud infrastructure services. Where in-scope services utilize cloud infrastructure services,

authorities would only be able to turn to the cloud infrastructure provider to enforce detection and removal orders as a measure of last resort.

What's Next?

In parallel, the CSAM Regulation is also being debated in the EU Council by representatives of the Member State governments. It is currently unclear when and in what form the Council of the European Union will be able to adopt its own position on the Commission draft—particularly due to concerns regarding the impact of CSAM detection orders on fundamental rights in certain EU Member States.

In any event, once the Council position is confirmed, trialogue negotiations among the Council, EP, and Commission will begin. As proposed by the Commission, the CSAM Regulation will enter into force six months after its final adoption.

Revised EU Product Liability Directive Addresses the Increase in AI and Online Shopping

In December 2023, negotiators from the European Commission, the EP, and the Council of the European Union reached a provisional (political) agreement[2] to revise the four-decades-old EU Product Liability Directive.[3]

The Product Liability Directive establishes a strict liability (i.e., non-fault-based) regime to allow claimants to seek compensation for defective products throughout the European Union, meaning that claimants do not need to prove fault to bring a successful claim.

What's New?

The provisional agreement addresses the increase in online shopping (also from outside the European Union) and the rise of new technologies (such as AI), as well as the need to ensure the transition to a circular economic model. To encourage innovation, the revised Product Liability Directive will not apply to open-source software developed or supplied as a noncommercial activity.

The new provisions are intended to ensure that there is always an EU-based entity (such as a manufacturer, importer, or their

authorized representative) that can be held liable for a product that causes damage, even if the product was not purchased in the European Union. In cases where such a liable company cannot be identified, the EP insisted that Member States should provide compensation through national compensation schemes.

The revised Product Liability Directive will clarify that information technology security vulnerabilities are a product defect and will extend the rules on strict liability to:

- Intangible products (including stand-alone software, digital content, Software as a service (SaaS), and AI applications),
- Damages caused by loss or corruption of data,
- Online marketplaces (under certain conditions), and
- Fulfilment services providers if they fail to promptly identify a relevant economic operator established in the European Union.

The new law will also improve the enforcement of civil law claims: by requiring disclosure of technical information to injured parties, allowing courts to presume that products are defective under certain circumstances, and reversing the burden of proof regarding the existence of a defect.

What's Next?

The text of the provisional agreement still has to be formally approved by the EP in plenary session (currently scheduled for April 2024) and then by the Council. After that, it will be signed and published in the *Official Journal of the European Union* and enter into force 20 days later. A 24-month transition period has been agreed, meaning that the new laws will enter into force in the first half of 2024 and apply from 2026.

Update on New EU Rules Promoting the Repair of Goods

The European Commission had adopted a new proposal for a Directive on common rules promoting the repair of goods[4] (the Proposed Directive) that will impose greater obligations on manufacturers of goods (including digital products) to repair defective products.

The Proposed Directive amends the remedies provided under the EU Sale of Goods Directive 2019/771 for nonconformity so that consumers will only be able to choose replacement as a remedy if it is cheaper than repairing the goods.

What's New?

The Commission's proposal has entered the EU legislative process, where it has been discussed within the EP and the Council, with both bodies proposing amendments to the proposal in preparation for trialogue negotiations:

- *Scope of the Obligation to Repair*:
  - *Commission*: Proposes repair obligations for manufacturers of products listed in Annex II with "reparability requirements" set by the Commission.
  - *Parliament*: Intends to extend this obligation to all producers of Annex II products, even those without defined "reparability requirements." This would give the Commission the right to add any product to Annex II.
- *Terms of the Obligation to Repair*:
  - *Commission*: Allows producers to choose the terms of repair (e.g., free or for a fee).
  - *Parliament and Council*: Add requirements like timely repairs. Parliament proposes offering a refurbished product as an alternative and mandates that the producers must provide repair information and spare parts to third-party repairers at fair costs.
- *Online Platform for Repair*:
  - *Commission and Parliament*: Encourage each Member State to set up an online platform for repairs and refurbished goods, covering more than Annex II goods.
  - *Council*: Prefers a single pan-European platform, allowing national platforms under certain conditions and including sellers of refurbished goods.
- *Liability Period*:
  - *Parliament*: Consumers must be provided with a temporary replacement if repair takes an unnecessarily long time; Parliament proposes to extend the statutory warranty period by twelve months once product is repaired.

- *Council*: Proposes to extend the warranty period by six months if repair is chosen, with sellers informing consumers of their rights and the extended period.

What's Next?

It is expected that the EP and the Council will reach an agreement and adopt the Proposed Directive before the EP elections in June 2024, so that the repairability requirements of the Directive could apply to products marketed in the EU/European Economic Area from 2026 to 2027.

Green Transition/Greenwashing: European Parliament Adopts New Law Banning Greenwashing and Misleading Product Information

The European Commission is planning—as part of the EU's Green Deal[5]—amendments to the Unfair Commercial Practices Directive (UCP) and the Consumer Rights Directive (CRD) to support the next steps toward a cleaner and greener EU economy. The EP has now adopted these amendments,[6] which are meant to interact with the Green Claims Directive, which is currently being discussed at the committee stage in the EP.

What's New?

Amendment of the UCP

The amendment of the UCP aims at further protecting consumers from misleading environmental claims and unreliable sustainability labels. In particular, general environmental claims like "environmentally friendly," "natural," "biodegradable," "climate neutral," or "eco" will be prohibited unless they can be properly evidenced.

Regarding the use of sustainability labels, the amendment only allows labels in the European Union that are based on "official certification schemes or established by public authorities." Finally, certain claims, according to which a product has a "neutral, reduced or positive impact on the environment because of emissions offsetting schemes," will be banned.

Amendment of the CRD

The amendment of the CRD is focused on durability of products. In particular, producers will have to make guarantee information more visible. Also, a new harmonized label for an extended guarantee period will be introduced to clearly provide such information to consumers. The amendment also addresses false claims on the repairability of goods.

What's Next?

After having reached a provisional agreement in the trialogue[7] and the latest adoption by the EP, the amendments of the UCP and the CRD now need final approval by the Council of the European Union. After that approval, the amendments will be published in the *Official Journal of the European Union*, and Member States will then have 24 months for implementation.

EU Implements Mandatory "Withdrawal Function" Requirement for Online Contracts

The European Commission issued a proposed Directive[8] in May 2022 that would, among other things, require traders to include a withdrawal button on the same electronic interface used to conclude consumer contracts—but only to facilitate the exercise of the 14-day right of withdrawal for financial services sold electronically.

In March and April 2023, the Council of the European Union[9] and the EP[10] adopted their positions on the Commission's proposed Directive. To further increase consumer protection, their positions propose to extend the application of the withdrawal button to all distance consumer contracts concluded through an online interface (e.g., websites or mobile apps)—thus going far beyond the Commission's original proposal.

What's New?

In the meantime, the Council and EP proceeded to formally adopt the legislation in October 2023, and the final Directive[11] was published in the *Official Journal of the European Union* in November 2023.

Based on its final wording, the Directive facilitates the exercise of the right to withdraw from any distance contract by requiring the service provider's interface to include a "withdrawal function" (now using broader terminology instead of "withdrawal button") that is easily readable and accessible to the consumer. The withdrawal function must allow the consumer to send an online notice of withdrawal informing the trader of their decision to withdraw from the contract. Traders must also send to consumers an acknowledgement of receipt of the withdrawal without undue delay and on a durable medium, including its content and the date and time of its transmission. The consumer will be deemed to have exercised the right of withdrawal within the 14-day withdrawal period if they have sent the online declaration of withdrawal before the expiry of that period.

The objective of this withdrawal function is to raise consumers' awareness of their rights of withdrawal and to ensure that it is as easy to withdraw from a contract as it is to conclude it. The withdrawal function is applied to all contracts concluded at a distance, not only financial services contracts.

What's Next?

The Directive must be transposed into the national laws of the Member States by December 2025. Its full application will start on June 16, 2026.

EU Finalizes Negotiations on New Rules for Political Advertising

In November 2023, the EU institutions reached an agreement[12] on the proposed new rules regarding political advertising in the form of a "Regulation on the Transparency and Targeting of Political Advertising."

The Regulation recognizes that political advertising is a growing and increasingly cross-border business—particularly due to the use of digital ad-tech solutions. To combat disinformation, it aims to ensure that political advertising is as transparent as possible, including in terms of relevant targeting and ad delivery techniques.

Once in force, these new rules will apply to political ads regardless of the relevant distribution channels, but they will have a

particular impact on online services where political ads may be placed.

What's New?

The Regulation applies to anyone providing political advertising services across the entire value chain from preparation through dissemination of political ads—but it specifically targets publishers of political ads, that is, services publishing, delivering, or disseminating such ads (such as social networks, broadcasters, ad networks). Its substantive rules essentially focus on provisions regarding ad transparency and related due diligence and on obligations regarding targeting and ad delivery techniques.

- In terms of transparency obligations, the Regulation aims to ensure that it is apparent whether advertising qualifies as a political ad. For each political ad, it must further be transparent on whose behalf it is published, who financed it, what was paid in exchange for it, and where those funds came from. For all political ads published in the European Union on "very large online platforms" designated under the EU Digital Services Act, this information will also be available in a public repository of political ads.
- In the context of political ads, the Regulation will only allow the use of targeting and ad delivery techniques that involve the processing of personal data (e.g., cookies) under specific conditions, including a political ad–specific consent requirement, and a ban on profiling based on sensitive personal data. In addition, further transparency requirements apply where political advertising facilitates such techniques, particularly requiring information on targeting logic and parameters.

What's Next?

The finalized wording of the Regulation will now need to be formally adopted by the EP and the Council of the European Union before it can be published in the *Official Journal of the European Union* and enter into force. Once that is done, it will apply subject to an 18-month transitional period—that is, in any event, after the next European elections in June 2024.

EU Finalizes Its New European Media Freedom Act

In December 2023, the EU institutions agreed on the final wording for the new European Media Freedom Act (EMFA).

The EMFA is an EU regulation that aims to harmonize and enhance EU rules on media pluralism, increase cross-border cooperation among media regulators, and address public and private interference with media outlets.

What's New?

The final EMFA wording still addresses all five categories of media entities contemplated by the original Commission draft in 2022, but it introduces some significant changes compared to that draft.

1. Providers of media services will enjoy further protection against state interference and unfair allocation of state advertising. This includes audiovisual and audio-only linear and on-demand offerings as well as press publications. However, media services with news and current affairs content will become subject to new obligations aimed at ensuring the editorial independence of relevant staff.
2. Manufacturers of devices and developers of user interfaces for audiovisual media services will have to implement functionalities so that users can change the default settings controlling or managing access to and use of such services. New wording added during the legislative process also requires them to respect the visual identity of the available media services.
3. Providers of "very large online platforms" as defined under the EU Digital Services Act will have to implement functionalities allowing users to self-declare that they are a media service under the EMFA. The very large online platform will then be subject to specific content moderation rules regarding content provided by declared media services. The final wording limits those specific rules to moderation measures aimed at enforcing the platforms' terms (i.e., excluding moderation of illegal content).
4. Providers of audience measurement systems will be subject to general nondiscrimination and transparency obligations,

and they may have to disclose their methodologies upon request. The final wording also added an audit obligation for audience measurement systems that are not based on industry standards.

5. Providers of video-sharing platforms will not become subject to new substantive rules, but the EMFA facilitates cross-border enforcement of existing regulations for relevant services.

What's Next?

The finalized wording of the regulation will now need to be formally adopted by the EP and the Council of the European Union before it can be published in the *Official Journal of the European Union* and enter into force. Once that is done, it will apply subject to a 15-month transitional period—that is, most likely at some point in 2025.

EU Adopts Its Data Act

The EU Data Act was first proposed in February 2022 as part of the European Commission's strategy for data, and came into force in January 2024.

What's New?

The Data Act was published in the *Official Journal of the European Union* on December 22, 2023, which means that it came into force on January 11, 2024, and its provisions will become fully applicable as of September 12, 2025. The Data Act:

- Introduces harmonized rules on fair access to and use of data in connection with Internet of Things products and related services,
- Enables users to switch more easily between different providers of data processing services, and
- Facilitates the interoperability of data, data-sharing mechanisms and services, and common European data spaces.

The Data Act also applies to business-to-business relationships and, therefore, is not just a consumer-focused piece of legislation.

Some highlights of the Data Act's provisions are the following:

- Connected products and related services (for example, as provided through mobile apps or SaaS) put on the market after September 12, 2026, will need to be designed, manufactured, and provided in a way that allows the user, where technically feasible, to directly access the product/service data that they generate by using such devices.
- Where data is not directly accessible by the user in such a way, the user can claim access to the "readily available" data from the data holder and request that it be shared with other data recipients.
- A data holder can only use and share the product/service data based on a contract entered into with the user.
- The Data Act prohibits certain unfair contractual terms if they are unilaterally imposed by one contract party on the other, such as a limitation on liability for intent or gross negligence.
- Certain public-sector bodies can request access to the data held by private companies in cases of public emergencies or for specific public interest purposes.
- The Data Act imposes obligations on data processing services (such as infrastructure as a service, platform as a service, or SaaS providers using shared resources for multiple customers) to ensure interoperability and enable users to switch from one provider to another more easily. While most obligations will only apply as of September 12, 2025, the restriction that the switching charge must not exceed the respective costs incurred by the provider is already applicable as of January 11, 2024. By January 12, 2027, providers of data processing services must not impose any switching charges on the customer for the switching process.

What's Next?

The Data Act will become fully applicable as of September 12, 2025, without further implementation steps by the EU Member States being necessary.

The Commission will need to produce some further documents and guidance, such as model contract clauses on data access and use, certain delegated acts, as well as harmonized standards regarding interoperability in relation to data sharing and data processing.

EU Reaches Provisional Agreement on a Cyber Resilience Act

The Council of the European Union, in coordination with the EP, has provisionally agreed to a proposed Cyber Resilience Act.

This legislation is a pivotal development in ensuring cybersecurity of digital products within the EU's single market. It represents a significant step in harmonizing cybersecurity standards across the European Union and underscores the increasing importance of digital security in product design and distribution.

What's New?

Key points of interest for legal practitioners and businesses include:

- *Scope and Objectives*. The Cyber Resilience Act introduces comprehensive EU-wide cybersecurity requirements for digital products, covering the entire life cycle from design to market availability. It encompasses all connected hardware and software products, with specific exemptions for products already regulated under existing EU cybersecurity laws.
- *Manufacturer Responsibility*. Central to the Cyber Resilience Act is the shift in compliance responsibility to manufacturers. They must undertake cybersecurity risk assessments, provide declarations of conformity, and engage in continuous cooperation with competent authorities. Additionally, manufacturers are responsible for maintaining robust vulnerability handling processes.
- *Consumer and Business Transparency*. The Cyber Resilience Act enhances transparency, enabling consumers and businesses to make informed decisions based on the cybersecurity features of digital products.

- *Co-Legislator Amendments*. Notable amendments include a simplified classification methodology for digital products, a defined support period of at least five years, and reinforced reporting obligations for actively exploited vulnerabilities. The role of the European Union Agency for Cybersecurity is notably strengthened in this context.

What's Next?

The final text is undergoing technical refinement and will require formal adoption once it has been through the trialogue process.

The Cyber Resilience Act will take effect three years post-enactment, allowing sufficient time for manufacturers to comply with the new requirements. Special provisions are made to support small and micro enterprises through awareness, training, and testing procedures.

EU Right to Withdraw from Auto-Renewing Subscription Contracts

The EU's top court has ruled on a consumer's right to withdraw from auto-renewing subscription contracts under the Consumer Rights Directive.

What's New?

In *Verein für Konsumenteninformationen v. Sofatutor*,[13] the European Court of Justice (ECJ) was asked to consider a contract for the performance of services that provided for an initial free period for the consumer after which—unless the consumer terminates or withdraws from that contract during that period—payment is required for a period that is automatically extended for a fixed term.

The ECJ ruled that a consumer's right to withdraw from a distance contract under the Consumer Rights Directive only applies once, at the start of the contract, and not when the free trial ends or the subscription auto-renews. So, there is no additional right of withdrawal at the conclusion of the free subscription period or when the free subscription converts to a regular, paid subscription.

However, this only applies if, at the time the contract is concluded, the trader has informed the consumer (in a clear, comprehensible, and explicit manner) that payment will be required for these services after the initial free period. Otherwise, the consumer does have a further right of withdrawal at the time of conversion to a regular, paid subscription.

What's Next?

This ruling limits consumers to a single right of withdrawal, applicable only at the start of the initial free period.

Companies using auto-renewal should be able to avoid cancellations at the time of transition to a paid subscription, provided they comply with the communication requirements.

However, failure to inform customers properly about the payment terms that will apply after the free period could lead to an increased risk of customers exercising their right of withdrawal upon conversion to a paid subscription.

Therefore, this decision places a greater emphasis on clarity and transparency in the terms of service, which could lead to adjustments in how subscription contracts are structured and communicated.

Germany

Updated Draft Legislation for OS-Level Youth Protection Settings

In November 2023, the Federal Republic of Germany presented for public consultation an updated draft for their revision of the German Youth Protection State Treaty.

The revision, which was originally proposed in mid-2022, aims to enable parents to more easily set up parental controls at a central location on their own (and their children's) devices to restrict access to inappropriate apps.

What's New?

The draft still requires operating systems (OS) for media devices to feature a specific parental control mechanism that allows users

to block unsuitable apps. However, the in-scope OS will now have to be designated by the regulator, so that the proposed rules would no longer be self-executing.

On in-scope OS, the new parental control mechanism will allow parents to set a device-wide age level (6, 12, 16, or 18) and it will block access to and installation of apps with an age rating higher than that age level. To facilitate this mechanism, the relevant system app store must collect age ratings for all available apps. The parental control mechanism must also deactivate app installations from non-system app stores, noting that the updated draft now permits such third-party app stores if they have a similar age-rating mechanism.

Apps that have their own built-in youth protection mechanisms are privileged. These apps must be made available regardless of the OS-level age setting. For such apps, the new draft also dropped the prior requirement of such apps having to automatically configure their internal mechanisms in accordance with the OS-level age setting.

What's Next?

The Federal Republic of Germany will now digest the input received during the consultation process and might then agree on a final wording for the new law. The law must then be ratified by all 16 State parliaments before it can enter into force. This will likely not happen before early 2025 and, judging from the pace of the legislative procedure to date, it may take even longer.

United Kingdom

UK Online Safety Act Imposes Greater Compliance Burden on In-Scope Digital Providers

The UK's controversial and long-awaited Online Safety Act (OSA) finally received Royal Assent in October 2023.

The OSA—which is intended to make the internet a safer place—comes with many additional duties and a greater compliance burden for in-scope companies (which includes user-to-user services like social media sites, content-sharing sites, online and mobile gaming services, and search services).

What's New?

The UK's communications regulator (Ofcom) has confirmed that it intends to take a phased approach to enforcement, with the first stage of new OSA-related duties to take effect in late 2024—but it is urging in-scope (and potentially in-scope) businesses to start preparing now, and also to "have their say" by engaging with Ofcom's consultations (including an ongoing consultation[14] on its proposals for protection from online illegal harms, which was due to close on February 23, 2024).

What Should Affected Entities Be Thinking About?

When the OSA is fully in force, in-scope businesses will essentially need to "assess and manage risks" to their users' online safety. This includes obligations to address user safety in your terms of service, and have adequate reporting and complaint systems in place for users—all while balancing safety measures against freedom of expression and right to privacy.

According to Ofcom's draft codes of practice, certain "large services"—currently defined as those with an average user base of 7 million or more per month in the United Kingdom—will likely have additional obligations to comply with, such as the use of specific tools to detect certain types of content on their services, and staff training and internal codes of conduct on protection from illegal harms.

What Can Affected Entities Do in the Meantime?

- Consider whether or not you might be in scope for the OSA obligations and, if so, start to think about the ways in which illegal harms could take place on your service for the purposes of carrying out any mandated risk assessments under the OSA.
- Engage with Ofcom's consultations to help ensure that the industry's concerns are being considered when shaping the codes of practice that will ultimately inform Ofcom's approach to compliance and enforcement.
- Calculate your number of monthly UK users to see if you could be a "large service" and therefore be subject to additional obligations.

What's Next?

The rules are yet to come into force (pending secondary legislation from the UK Secretary of State and the publication of codes of practice by Ofcom) but businesses are being encouraged to start engaging with the OSA now.

UK Online Fraud Charter: Fraud Protection Beyond the Online Safety Act

Major tech companies have signed an agreement with the UK government—called the Online Fraud Charter[15]—to enhance protection against online fraud. The Charter is designed to complement the OSA (and its related codes of conduct) as part of the UK government's wider Fraud Strategy.[16]

What's New?

While commitment to the Charter is voluntary, by signing up, companies agree to adopt certain antifraud measures within six months of the Charter's publication (i.e., before the end of May 2024). The Joint Fraud Taskforce will then hold these companies accountable for their implementation of the Charter.

The Charter's list of actions will only apply to companies on a proportionate basis, so the entire list will not apply to every company or in every circumstance, and the Charter sets out which types of companies are expected to implement which specific actions. However, the overarching commitments for companies to implement are as follows:

- *Blocking*. Deploying measures to detect fraudulent material.
- *Reporting*. Using quick and simple mechanisms for reporting fraudulent material.
- *Takedowns*. Immediately taking action against fraudulent content and users.
- *Advertising*. Deploying measures to protect individuals from fraudulent ads.
- *Law Enforcement*. Using dedicated liaisons to respond to law enforcement requests.
- *Intelligence Sharing*. Engaging with initiatives to quickly share information about fraud.

- *Transparency*. Sharing information about fraud risks and how they are addressed.
- *Communications*. Delivering simple messaging to help users recognize and avoid online fraud.
- *Horizon Scanning*. Contributing to horizon scanning exercises.

How Does the Charter Work with the OSA?

The Charter is a separate and distinct framework that is geared toward targeting a smaller subset of online platforms and services compared to the OSA. This means that that fulfilment of Charter obligations will not necessarily mean fulfilment of a company's fraud-related OSA duties, and so each framework should be approached separately.

What's Next?

The OSA will take precedence if there is any direct conflict with the Charter and the UK government plans to keep the Charter under review to ensure that its commitments do not duplicate or diverge from other regulatory requirements (including Ofcom's future Codes of Practice).

UK Government Opens Consultation on Newly Proposed Security Standards for Data Centers

The UK government is proposing a new statutory framework[17] (the Framework) for UK-based third-party data center services and is seeking views on the proposed Framework.

The government is particularly keen to receive feedback from parties such as cloud platform providers, managed service providers, data center operators, data center land and facility owners, and the customers and suppliers of these parties.

What's New?

The Framework will target organizations that operate data centers, particularly those that provide collocation and cohosting data center services as a third-party provider.

This will include data centers that have other functions or services outside collocation or cohosting. However, data center services or parts of data centers that fall solely under:

- Public electronic communications services and networks,
- Digital infrastructure,
- Enterprise data storage and processing,
- Cloud services,
- Managed services, and
- Submarine or subsea fiber optic cables will likely be out of scope (but still potentially subject to other regulations such as the UK's Network and Information System Regulations 2018).

More broadly, in its proposal, the UK government acknowledges that some parts of the data center sector will already fall under the UK's critical national infrastructure. The government is therefore also considering whether third-party data center infrastructure should be a subsector of the critical national infrastructure, which is governed by its own separate regime.

What Are the Key Takeaways?

The Framework sets out proposed obligations for in-scope organizations, including:

- *Registration*. Registering with the designated regulator and providing relevant information regarding an organization's UK operations.
- *Security and Resilience Measures*. Taking appropriate and proportionate technical and organizational measures to manage risks or security and resilience of data center services. This will include implementation of certain baseline measures for areas such as risk and incident management, resilience and service continuity, governance and personnel, and supply chain management.
- *Incident Reporting*. Reporting significant incidents to the regulator and in some cases, disclosing incidents to customers and other affected parties such as suppliers.

The Framework also suggests the establishment of (1) a new regulatory function to enforce the Framework, and (2) new

standards, assessment frameworks, and other tools for a regulator to use to ensure that organizations have implemented baseline security and resilience measures. However, the government stopped short of proposing the establishment of a new regulatory body or identifying an existing regulatory body to enforce the Framework.

What's Next?

The consultation closed on February 22, 2024.

Notes

* The authors, attorneys with Morrison Foerster's European Digital Regulatory Compliance team, may be contacted at amaughan@mofo.com, agruenwald@mofo.com, cwalker-osborn@mofo.com, cnuessing@mofo.com, and sashcroft@mofo.com, respectively.

1. https://www.europarl.europa.eu/doceo/document/A-9-2023-0364_EN.html.
2. https://www.europarl.europa.eu/news/en/press-room/20231205IPR15690/deal-to-better-protect-consumers-from-damages-caused-by-defective-products.
3. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31985L0374.
4. https://commission.europa.eu/document/afb20917-5a6c-4d87-9d89-666b2b775aa1_en.
5. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_en.
6. https://www.europarl.europa.eu/news/en/press-room/20240112IPR16772/meps-adopt-new-law-banning-greenwashing-and-misleading-product-information.
7. https://www.consilium.europa.eu/en/press/press-releases/2023/09/19/council-and-parliament-reach-provisional-agreement-to-empower-consumers-for-the-green-transition/.
8. https://eur-lex.europa.eu/resource.html?uri=cellar:e7cebe9a-d208-11ec-a95f-01aa75ed71a1.0001.02/DOC_1&format=PDF.
9. https://data.consilium.europa.eu/doc/document/ST-7037-2023-INIT/en/pdf.
10. https://www.europarl.europa.eu/doceo/document/A-9-2023-0097_EN.html.
11. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302673.

12. https://data.consilium.europa.eu/doc/document/ST-17037-2023-INIT/en/pdf.

13. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0565.

14. https://www.ofcom.org.uk/consultations-and-statements/category-1/protecting-people-from-illegal-content-online.

15. https://assets.publishing.service.gov.uk/media/65688713cc1ec5000d8eef96/Online_Fraud_Charter_2023.pdf.

16. https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf.

17. https://assets.publishing.service.gov.uk/media/657ab6f6254aaa000d050ce2/protecting_and_enhancing_the_security_and_resilience_of_UK_data_infrastructure.pdf.