TDL | Trust in Digital Life

European Proposals, Regulations and Initiatives Update

16 May 2023

TDL | Trust in Digital Life

European Proposals, Regulations and Initiatives Update

Table of contents

Proposals

European Approach to Artificial Intelligence (AI Act)

According to a source in the media, MEPs have reached an agreement at the technical level regarding key outstanding issues on the AI Act proposal.

Several technical (non-public) meetings were scheduled by the European Parliament throughout the end of March and April in an effort to find agreements on key remaining obstacles to the proposed AI Act.

According to EURACTIV, MEPs reached a provisional political agreement at the technical level on 27 April, the main elements of which can be summarised as follows.

- With regard to general purpose AI, MEPs agreed to place stricter obligations on the subcategory of foundation models. As for generation AI models, the compromise would stress that these must be designed and developed in accordance with EU law and fundamental rights.
- Concerning prohibited practices, a proposal to prohibit AI-powered tools for general monitoring of interpersonal communications was scrapped due to opposition from the EPP group. In its place, EPP MEPs accepted an extension on the ban on biometric identification software.
- Additionally, the compromise would ban the use of AI-powered emotion recognition software in the areas of law enforcement, border management, education, as well as in the workplace. A ban on predictive policing would also be extended from criminal offenses to administrative offenses under the compromise.
- Furthermore, MEPs agreed that AI systems listed under Annex III would only be considered high-risk if they pose a significant harm to health, safety, or fundamental rights. Additionally, AI systems used to manage critical infrastructure such as energy grids would also be considered as high-risk if they pose a severe environmental risk, as well as recommender systems of very large online platforms (VLOPs).
- Moreover, the compromise would include additional safeguards in cases where providers of high-risk AI models may process sensitive data to detect negative biases, specifically to prohibit the detection of biases through the processing of synthetic, anonymised, pseudonymised or encrypted data.
- Lastly, the compromise would: (i) apply the general principles of human agency and oversight, technical robustness and safety, privacy and data governance, as well as a few others to all AI models; (ii) oblige high-risk AI systems to record their environmental footprints; and (iv) require foundational models to comply with EU environmental standards.

Following the IMCO-LIBE Committees' adoption of the Report (consolidated text not yet publicly available) on 11 May, the text is now expected to be sent to plenary for formal adoption. A debate and vote in plenary on the Report of the joint lead IMCO-LIBE Committees is tentatively scheduled to take place on 13 June 2023.

Next Steps

Council

As the Transport, Telecommunications, and Energy (TTE) Council adopted the Council's negotiating mandate (General Approach) on 6 December 2022, the launch of informal trilogue negotiations is pending the European Parliament's adoption of its own position.

European Parliament

Rules 57 (Associated Committee) and 58 (Joint Committee procedure) of the European Parliament's Rules of Procedure apply to this proposal.

Under those Rules, the European Parliament's IMCO and LIBE Committees (Lead) and ITRE, JURI, and CULT Committees (Associated) work in close cooperation. The Joint Lead Committees will have to accept, without a vote, the amendments proposed by the Associated Committees on the topics that fall within their respective exclusive competences.

According to a report by EURACTIV, the IMCO-LIBE Committees are tentatively scheduled to vote on the joint draft Report, as well as the amendments tabled to it, on 11 May 2023. Once approved, the Committees would then submit their joint text to plenary for adoption, possibly during the week of 12-15 June 2023. The approved text would constitute the European Parliament's negotiating position.

The JURI Committee adopted its Opinion on 5 September 2022, the ITRE Committee adopted its Opinion on 14 June 2022 and the CULT Committee adopted its Opinion on 15 June 2022.

Trilogues

On the basis of the negotiating position of the European Parliament and the Council's General Approach, trilogues between the two institutions would start, possibly in late June or early July 2023. During the trilogue negotiations, the European Parliament and the Council would aim to reach a first reading agreement on the proposal. The agreed text would then be published in the EU Official Journal before entering into force.

Cryptocurrencies

The Council's Permanent Representatives Committee (COREPER) endorsed the adoption of the European Parliament's position on the proposal for a Regulation on markets in crypto-assets (MiCA) on 10 May 2023.

The European Parliament's position reflects the compromise agreed by both institutions reached through trilogue negotiations. The proposal is tentatively scheduled to be voted upon by Member States Ministers without debate (as an "A" item of the agenda) at the ECOFIN Council meeting to be held on 16 May, resulting in the formal adoption of the text.

Once adopted by the Council, the legislative procedure would be concluded at first reading. The final text of the Regulation would then be published in the EU Official Journal before entering into force.

As the European Parliament adopted its first reading position (draft Regulation) on 20 April 2023, the Council is now scheduled to adopt the text during the Economic and Financial Affairs (ECOFIN) Council meeting on 16 May 2023.

The Council's Permanent Representatives Committee (COREPER) endorsed the text prior to its adoption by the ECOFIN Council, on 10 May 2023.

Once approved by the Council, the legislative procedure would be concluded at first reading. The final text (Regulation) would be published in the EU Official Journal and enter into force twenty days following its publication.

Cyber Resilience Act

The Permanent Representatives Committee (COREPER I) is scheduled to meet on 17 May 2023 to prepare for the upcoming Transport, Telecommunications, and Energy (TTE) Council, which is to take place on 1-2 June 2023.

MEPSs of the lead ITRE committee tabled 423 amendments to the draft Report and are now available. LIBE, which is an Associated Committee on the file, decided not to give an Opinion on the file. Therefore, it is no longer expected to appoint a Rapporteur or Shadow Rapporteurs, prepare a draft Opinion, or adopt a final Opinion on the proposal.

As the draft Report itself contains 123 amendments to the Commission's proposal, a total of 546 amendments have been tabled on the file by the ITRE Committee alone.

The main changes proposed by the amendments to each Chapter of the proposal can be summarised as follows:

Recitals (Amendments 124-203)

The amendments proposed for the recitals reflect the changes made within the Articles of the text.

Chapter I - General Provisions (Articles 1-9; Amendments 204-267)

With regard to the scope of the measure, it was underscored that the proposed Regulation should not apply to software provided under free and open source licences, except when such software is provided as a paid or monetised product.

In parallel, it was suggested that the proposed Regulation not apply to spare parts that are exclusively manufactured in order to repair products with digital elements that have been placed on the market before the application date of this measure.

Furthermore, definitions for the terms *'consumer product with digital elements'*, *'business-to-business product with digital elements'*, *'cybersecurity'*, *'software'*, *'consumer'*, *'provider of an online marketplace'*, *'substantial modification'*, *'near miss'*, *'incident'*, and *'significant cyber threat'* were modified or introduced by Shadow Rapporteurs.

In parallel, it was suggested removing the definitions for the terms *'critical products with digital elements'*, *'highly critical product with digital elements'*, and *'highly foreseeable misuse'*.

It was underscored that Member States should not prevent the presentation and use of a non-compliant prototype product with digital elements or a software, provided that the availability is limited in time and geographical area and is supplied exclusively for testing.

Additionally, changes were proposed to the Commission's ability to adopt delegated acts.

It was also proposed that internal networks of a machinery product with digital elements should not be subject to the proposed Regulation when they are secured via dedicated endpoints and isolated from external networks, and where the manufacturer assesses and indicates the intended final use of the component for the sole internal operations and communication.

Chapter II - Obligations of Economic Operators (Articles 10-17; Amendments 268-362)

Concerning the obligations of manufacturers, it was highlighted that manufacturers should ensure that components sourced from third parties do not compromise the security of the product with digital elements.

In addition, it was stressed that manufacturers should be obliged to determine the expected product lifetime, taking into account the time users reasonably expect to be able to use the product given its functionality and intended purpose.

Given this, it was emphasised that manufacturers should also publicly communicate and advertise the expected product lifetime of their products.

Furthermore, a new Article 10a was introduced outlining manufacturers' reporting obligations with regard to vulnerabilities. Amendments were also tabled specifying additional notification obligations.

Several Shadow Rapporteurs proposed amendments to Chapter II with a view to further align it with the NIS2 Directive.

Moreover, conditions were proposed under which an incident would be considered significant.

In parallel, a new Article 11a was inserted to oblige manufacturers to designate a single point of contact to enable users to communicate directly and rapidly with them.

Several provisions within Chapter II were modified in order to simplify them for SMEs. A new Article 17a was also introduced outlining specific obligations for providers of online marketplaces.

Chapter III - Conformity of the Product with Digital Elements (Articles 18-24; Amendments 363-385)

The areas in which the Commission should request the drafting of harmonised standards were specified and suggested removing Article 19 on common specifications from the text in its entirety. Additionally, several amendments were aimed to further align the text with the Cybersecurity Act.

Moreover, it was underscored that the Commission should ensure that appropriate financial support in the regulatory framework of existing EU programmes is allocated to SMEs in order to mitigate possible financial burden.

Chapter IV - Notification of Conformity Assessment Bodies (Articles 25-40; Amendments 386-394)

With regard to conformity assessment bodies, the Member States and Commission were called on to put in place appropriate measures to ensure sufficient availability of skilled professionals.

Chapter V - Market Surveillance and Enforcement (Articles 41-49; Amendments 395-436)

With respect to the supervision of the implementation of the reporting obligations under the proposed Regulation, it was stressed that designated market surveillance authorities should cooperate with ENISA. It was also highlighted that such authorities should facilitate the active participation of stakeholders in market surveillance activities.

Additionally, a new Article 41a was introduced establishing an expert group on technical matters, while a new Article 41a was inserted to ensure civil society participation in market surveillance activities.

In parallel, a new Article 49a was proposed to allow the Commission, ENISA, and Member States to establish European cyber resilience regulatory sandboxes with voluntary participation of manufacturers of products with digital elements.

A new Article 49a was also inserted to provide for the right to compensation for damage or loss.

Chapter VI - Delegated Powers and Committee Procedure (Articles 50-51; Amendments 437-442)

The amendments tabled to Chapter VI further specified the Commission's power to adopt delegated acts.

Chapter VII - Confidentiality and Penalties (Articles 52-53; Amendments 443-448)

With regard to penalties, several amendments focused on ensuring that the financial capabilities of SMEs are taken into account.

In addition, a new Article 53a was introduced to further specify the allocation of penalties.

Chapter VIII - Transitional and Final Provisions (Articles 54-57; Amendments 449-460)

Lastly, several Shadow Rapporteurs proposed new application dates of the proposed Regulation.

Annexes (Amendments 461-546)

The amendments made to the Annexes reflect the changes made within the Articles of the text.

Next Steps

Following its publication on 15 September 2022, the proposal was sent to the European Parliament and the Council for examination.

European Parliament

Rule 57 of the European Parliament's Rules of Procedure applies to this proposal. Under this rule, the ITRE (Lead) as well as the IMCO and LIBE (Associated) Committees are obliged to adhere to the principle of sincere cooperation and work alongside one another on the drafting of the European Parliament's position on the proposal within their respective areas of competence.

A vote in the Lead ITRE Committee on the draft Report, as well as the amendments tabled to it, is tentatively foreseen for 19 July 2023. Once approved, the Committee would then submit its text to plenary for adoption. However, a date for the vote in plenary has yet to be determined. The approved text would constitute the European Parliament's negotiating position.

The Associated IMCO Committee is tentatively scheduled to meet and discuss the amendments tabled to the draft Opinion on either 22 or 23 May 2023. A vote on the draft Opinion, as well as the amendments tabled to it, is then tentatively scheduled to take place on either 28 or 29 June 2023.

According to the European Parliament, the Associated LIBE Committee decided not to give an Opinion on the file. Therefore, it is no longer expected to appoint a Rapporteur or Shadow Rapporteurs, prepare a draft Opinion or adopt a final Opinion on the proposal.

Council

The Council's Horizontal Working Party on Cyber Issues will continue meeting over the coming months to examine the proposal and to prepare the Council's negotiating mandate (General Approach). Once finalised at the technical level, input on the political level could be given by Member State Ambassadors (COREPER) and Ministers. This General Approach would need to be endorsed by COREPER and possibly adopted in a Council configuration. The General Approach would serve as a basis for the inter-institutional negotiations with the Parliament.

Trilogues

On the basis of the negotiating position of the European Parliament and the Council's General Approach, trilogues between the two institutions would begin. During the trilogue negotiations, the European Parliament and the Council would aim to reach a first reading agreement on the proposal.

The agreed text would then be published in the EU Official Journal before entering into force. Under the Commission's proposed text, the measure would enter into force on the twentieth day following that of its publication. It would then apply 24 months after its entry into force, with the exception of the manufacturer reporting obligation, which is to become applicable from 12 months after the measure's entry into force.

Data Act

During a meeting scheduled for 17 May 2023, Member State Ambassadors will meet to prepare for the second round of interinstitutional negotiations (trilogue), which is scheduled to take place on 23 May 2023.

The lead ITRE Committee met on 25 April 2023 to be briefed on the outcome of the first round of trilogue negotiations on the Data Act proposal, which took place on 29 March 2023.

As the negotiations are still in early stages, the Rapporteur informed that the trilogue only consisted of a brief discussion of the main issues for each co-legislator. No further details were provided.

To conclude, it was confirmed that the second trilogue is scheduled to take place on 23 May, while the third trilogue is scheduled for 27 June. The Rapporteur also informed that the aim is to conclude negotiations under the current Swedish Presidency, indicating that the third trilogue may possibly serve as the last one on the file.

If the co-legislators reach a provisional agreement during trilogues, the text of the agreement will be submitted to the lead ITRE Committee for approval and then to the plenary for adoption.

Once adopted by MEPs in plenary, the text will be sent to Council for approval, first by the Permanent Representatives Committee (COREPER) and then by a subsequent Configuration for final adoption.

Once approved by both co-legislators, the agreed text would then be published in the EU Official Journal. Under the Commission's proposed text, the measure would enter into force on the twentieth day following that of its publication and apply twelve months after its entry into force.

Data Protection Law Enforcement Directive (LED)

The Commission presented its proposal for a Regulation amending Council Decision 2009/917/JHA as regards its alignment with Union rules on the protection of personal data on 11 May 2023.

The measure aims to amend Council Decision 2009/917/JHA to align it with the data protection rules laid down in Directive (EU) 2016/680 in order to provide a strong and coherent personal data protection framework in the EU.

Council Decision 2009/917/JHA establishes the Customs Information System (CIS), an automated information system for customs purposes, which aims to assist in preventing, investigating, and prosecuting serious contraventions of national laws by making information available more rapidly and increasing the effectiveness of the customs administrations.

Directive (EU) 2016/680 (the Data Protection Law Enforcement Directive or LED) applies to both domestic and cross-border processing of personal data by competent authorities for the purposes of preventing, investigating, detecting, or prosecuting criminal offences and executing criminal penalties, including safeguarding against and preventing threats to public security.

European e-ID (eIDAS 2.0)

Member States Ambassadors of COREPER I will meet to prepare for the second round of interinstitutional negotiations (trilogue) on the European Digital Identity proposal on 17 May.

The Council's Working Party on Telecommunications and Information Society was briefed by the Swedish Council Presidency on 10 May 2023 on the state of play of the ongoing informal trilogue negotiations on the European Digital Identity proposal.

An exchange of views on a document (not publicly available) regarding the state of play of the file is expected to follow the briefing.

According to a report by *EURACTIV*, the European Parliament is "growing frustrated at the Swedish Council Presidency" as progress on the file is proceeding very slowly, and that the negotiations will likely continue under the incoming Spanish Council Presidency, which will take over leadership on 1 July 2023.

Discussions thus far have mainly focused on the wallet, as well as relying parties and governance, while the issue of unique identifiers is expected to be examined during the next (second) trilogue which may take place towards the end of May. The first trilogue took place on 21 March 2023.

If the co-legislators reach an informal political agreement (provisional agreement) during the trilogues, the text of the agreement will be submitted to the ITRE Committee for approval and then to the plenary for adoption. Once adopted by MEPs in plenary, the text will be sent to Council for approval, first by the Permanent Representatives Committee (COREPER) and then by a subsequent Configuration for final adoption. Once approved by both co-legislators, the agreed text would then be published in the EU Official Journal. Under the Commission's proposed text, the measure would enter into force on the twentieth day following that of its publication.

e-Privacy

On 20 April, the Rapporteur informed via Twitter that the Swedish Council Presidency has still not responded to her letter (not publicly available), which was sent on 6 March 2023.

As previously reported, the letter urged the Swedish Council Presidency to accelerate work on the ePrivacy file as it has been "almost a year since the last political trilogue meeting" and because she considered it crucial that the co-legislators "make progress on this legislative act, as it will have a significant impact on the fundamental rights of individuals and the future of digital communication in Europe".

The letter also invited the Presidency to arrange a subsequent trilogue to share its insights in order to finalise negotiations. The Rapporteur specifically pushed for the next trilogue to take place on either 25 April or 10 May 2023.

However, given that the Swedish Presidency has yet to respond, a subsequent trilogue is now considered unlikely to happen.

The Commission may withdraw the proposal soon if no further action is taken on the file. More information regarding the next steps may be announced in the coming weeks.

Next Steps

The Commission indicated in its 2023 Work Programme that the proposal will be part of the Commission's priority pending files for 2023.

As the Council and European Parliament respectively adopted their General Approach and negotiating position, informal interinstitutional negotiations (trilogues) between the co-legislators have been taking place with a view of reaching an agreement.

The first round of trilogues took place on 20 May 2021, whereas the second round took place on 18 November 2021. After several months of deadlock, the third trilogue took place on 31 March 2022.

After a year since the last trilogue, a source in the media reported that the Rapporteur sent a letter (not publicly available) to the Swedish Council Presidency urging it to accelerate work in order to conclude the negotiations on the file. As a result, she invited the Presidency to arrange a subsequent trilogue, possibly on either 25 April or 10 May 2023.

However, on 20 April 2023, the Rapporteur informed via Twitter that the Presidency had not responded to her letter. Given this lack of response, a subsequent trilogue is now considered unlikely to happen.

If no agreement can be reached and/or no further action is taken on the file, then the Commission will withdraw or amend the text.

If, however, the Council and the Parliament reach an agreement, the resulting compromise would need to be approved by both parties through their respective internal procedures.

The text of the agreement would first be sent to the European Parliament's LIBE Committee for approval and then to plenary for adoption.

Once adopted by MEPs in plenary, the text would then require the formal approval of the Council, first by the Permanent Representatives Committee (COREPER), and then in a subsequent Configuration meeting for final adoption.

Following the approval of the Council, the procedure would be concluded at first reading. As such, the Regulation would be published in the EU Official Journal and would enter into force twenty days following that of its publication.

EU Interoperability Framework

The Permanent Representatives Committee (COREPER I) is scheduled to meet on 17 May 2023 to prepare for the upcoming Transport, Telecommunications, and Energy (TTE) Council, which is to take place on 1-2 June 2023.

On 23 May 2023 the LIBE Committee, which is an Associated Committee on the file will discuss its draft Opinion on the Interoperable Europe Act proposal.

Following its publication on 18 November 2022, the proposal was sent to the European Parliament and the Council for examination.

European Parliament

Rule 57 of the European Parliament's Rules of Procedure applies to this proposal. Under this rule, the ITRE (Lead) and LIBE (Associated) Committees are obliged to adhere to the principle of sincere cooperation and work alongside one another on the drafting of the European Parliament's position on the proposal within their respective areas of competence.

ITRE (Industry, Research, and Energy) MEPs had until 3 May 2023 to table amendments to the draft Report. The text of the amendments is expected to be made publicly available in the coming weeks. The Committee is then expected to vote on the draft Report and amendments, once the Associated Committee has adopted its Opinion. Once approved, the Committee would then submit its text to plenary for adoption. The approved text would constitute the European Parliament's negotiating position.

The Associated LIBE Committee (Civil Liberties, Justice, and Home Affairs) is scheduled to discuss its draft Opinion on 23 May 2023, following which LIBE MEPs will have until 26 May 2023 to table amendments to the text.

A vote on the draft Opinion and the amendments tabled to it would then subsequently take place.

Council

The Council's Working Party on Telecommunications and Information Society is expected to continue meeting over the coming months to examine the proposal in order to prepare the Council's negotiating mandate (General Approach). Once finalised at the technical level, input on the political level could be given by Member State Ambassadors (COREPER) and Ministers. This General Approach would need to be endorsed by COREPER and possibly adopted in a Council configuration and would serve as a basis for the inter-institutional negotiations with the Parliament.

Trilogues

On the basis of the negotiating position of the European Parliament and the Council's General Approach, trilogues between the two institutions would begin. During the trilogue negotiations, the European Parliament and the Council would aim to reach a first reading agreement on the proposal. The agreed text would then be published in the EU Official Journal before entering into force. Under the Commission's proposed text, the measure would enter into force on the twentieth day following that of its publication. However, it would only start to apply three months thereafter.

Open Finance Framework

The Commission is tentatively scheduled to present its proposal for a Regulation on an open finance framework in late June. A version of the College of Commissioners' upcoming agenda for the first half of 2023 was leaked in the media on 11 January 2023.

The Commission had previously indicated in its 2023 Work Programme that the upcoming proposal for a Regulation on an open finance framework was scheduled for presentation during the second quarter of 2023.

According to a leaked agenda for the College of Commissioners' weekly meetings to be held during the first half of 2023, the Commission is expected to present the proposal on 28 June 2023.

As the leaked agenda is not an official document, the timeline for the presentation of the initiative remains tentative and may be subject to change.

Regulations

Digital Operational Resilience for Financial Sector (DORA)

The Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) entered into force on 16 January 2023 amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014, and (EU) 2016/1011 entered into force on 16 January 2023.

The Regulation was published in the EU Official Journal on 27 December 2022 and applies from 17 January 2025.

Digital Services Act (DSA)

Following its publication in the EU Official Journal on 27 October 2022, the Regulation on a Single Market For Digital Services amending Directive 2000/31/EC (Digital Services Act) entered into force on 16 November 2022 and will apply from 17 February 2024. However, Articles 24(2), 24(3), 24(6), 37(7), 40(13), 43, and Sections 4, 5, 6 of Chapter IV applied from 16 November 2022.

The Regulation establishes new rules to ensure the protection of the digital space against the spread of illegal content, as well as the protection of users' fundamental rights, as it defines clear responsibilities and accountability for providers of intermediary services.

In addition, the Regulation amends Directive 2000/31/EC (the Electronic Commerce Directive) by deleting its Articles 12-15 regarding the liability of intermediary services. References to these deleted provisions will now refer to Articles 4, 5, 6, and 8 of the DSA regarding the same subject.

The Regulation also amends Directive (EU) 2020/1828 by adding a reference to the DSA in its Annex I, which outlines the list of provisions of Union law referred to in Article 2(1) of the Directive concerning its scope.

General Data Protection Regulation (GDPR)

The European Data Protection Board (EDPB) regularly issues Guidelines, which aim to provide guidance on the application of provisions within Regulation 2016/679, also known as the General Data Protection Regulation (GDPR).

As such, the EDPB often launches public consultations on its draft Guidelines in order to take stakeholder feedback into account before finalising them.

Once the draft Guidelines and Recommendations are finalised, they may be adopted by the EDPB during its plenary sessions.

With regard to the Guidelines for which public consultations have recently closed, the EDPB will examine the feedback received while finalising the texts in the coming months.

The EDPB's 6-week public consultation (external link) on draft Recommendations 01/2022 on the Application for Approval and on the elements and principles to be found in Controller Binding

Corporate Rules (Article 47 GDPR) was launched on 17 November 2022 and closed on 10 January 2023.

The feedback submitted by stakeholders has not been made publicly available at this stage, however, the EDPB may decide to publish the comments in the coming weeks.

The draft Recommendations suggest that the current BCR-C reference, which contains standards for BCR-C approval, be updated and combined with the BCR-C standard application form. The updated Recommendations expand on the agreements reached by data protection authorities during approval processes for specific BCR applications following the implementation of GDPR. They offer more guidance and aim to make the process fairer for all BCR candidates.

More specifically, these Recommendations aim to:

i. Supply controllers with a common application form to use when requesting approval of their BCR-Cs.

ii. Explain the essential elements of BCR-C as stipulated in Article 47 GDPR.

iii. Distinguish between what should be included in the BCR-C and what should be submitted to the BCR Lead supervisory authority in the BCR application; and

iv. Provide clarifications and feedback on the requirements.

The Recommendations are accompanied by Annexes, which provide guidance for the application. Following the closure of the public consultation, the feedback received will now be examined by the EDPB while finalising the text in the coming months.

Initiatives

European Health Data Space

On 23 May, MEPs of the European Parliament's ITRE Committee are scheduled to vote on the Rapporteur's draft Opinion on the proposal for a Regulation on the European Health Data Space (EHDS), whilst Council experts will discuss the Swedish Presidency's second compromise text (not yet publicly available) on the same day. The vote was previously expected to take place in June 2023.

This means both associated Committees, the ITRE Committee and the Committee on Internal Market and Consumer Protection (IMCO), would be expected to adopt their respective Opinions on that day.

The Council Working Party on Public Health is scheduled to discuss the Swedish Council Presidency's second compromise text (not yet publicly available) on the file on 23 May 2023.

The proposal follows the ordinary legislative procedure (previously co-decision) under the Lisbon Treaty. Therefore, following its publication on 3 May 2022, the proposal was sent to the European Parliament and the Council for examination.

Virtual Worlds (Metaverse)

The Commission's four-week public consultation (external link) on its call for evidence for an initiative (without an impact assessment), which was launched on 5 April, closed on 3 May 2023 with a total of 169 comments submitted by stakeholders.

The feedback consisted of 42 comments came from EU citizens, 32 from business associations, 30 from companies/business organisations, 25 from non-governmental organisations (NGOs), 18 from stakeholders marked as 'other', 9 from academic and research institutions, 6 from public authorities, 3 from consumer organisations, 2 from trade unions, 1 from an environmental organisation and 1 from a non-EU citizen.

The main comments can be summarised as follows:

(1) Non-governmental organisations (NGOs)

The Alliance to Counter Crime Online stressed the need to ensure that safe design principles of virtual worlds are regulated before such products are released to the public, not after. Additionally, the organisation called for online businesses to face the same liabilities as other stores for hosting illicit activities, so that they are required to restrict and remove criminal activities.

The Open Future Foundation called for:

i. policymakers to prioritise public interest in policy debates to acknowledge virtual worlds as more than just services offered by commercial enterprises.
ii. open standards to be implemented to achieve interoperability between virtual worlds.
iii. data governance to be required so that virtual worlds are governed as digital commons; and
iv. the EU to invest in virtual worlds to ensure they are not only developed by private firms and that they also serve as digital public spaces.

Defend Democracy argued that the only responsible approach to virtual worlds is to use the precautionary principle, given that strong regulatory frameworks have already failed to protect democracy or mental health. They stressed that virtual worlds should only be developed with strict product safety requirements.

(2) Companies/Business Organisations

3DBear believed that the EU could become a leader in metaverse technologies if it facilitated the ecosystem and brought important players together, initiated funding and found synergies between public and private entities, enabled innovative public procurement, and had flexibility in regulation for pilot programmes and the development of new solutions.

They argued that EU metaverse policy should:

i. allow anyone the ability to create their virtual world.
ii. ensure interoperability and avoid closed metaverses; and
iii. address AI-generated and -assisted virtual worlds.

The industrial metaverse is key for Siemens calling on the Commission to:

i. distinguish between business-to-business (B2B) and business-to-consumer (B2C) use cases.
ii. stimulate and accelerate the uptake of digital technologies in the EU.
iii. facilitate a strong international standardisation effort.
iv. focus on next-generation networks and connectivity.
v. facilitate global collaboration among industry players; and
vi. focus on IP protection and work to prevent a shortage of skilled workers.

TikTok emphasised that the EU could become a thought leader to create virtual worlds that are value-driven. In addition, the company stressed the importance of interoperability and ensuring the protection of users' identities by interlinking virtual worlds with existing EU legislation such as the GDPR or the DSA. TikTok also called for policymakers to identify responsibilities and obligations relating to virtual worlds for areas such as user safety, liability, data protection, security, and IP protection.

Epic Games underscored that the metaverse should be based on an open economy in which all creators and developers can participate on equal terms and be rewarded for their contributions. The company also stressed the importance of interoperability and ensuring the proper enforcement of the DMA, so that companies such as Apple and Google are prevented from acting as gatekeepers for developers of virtual worlds.

(3) Business Associations

ETNO and GSMA welcomed the Commission's decision to opt for a non-legislative instrument, as they considered that it is too early in the technology development cycle to set binding rules for virtual worlds. Additionally, the associations argued that investments from telecommunication operators to ensure gigabit connectivity should be supported by the Commission. They also called for legal consistency with other European legislation, including the GDPR, DSA and DMA.

Bitkom supported the initiative on virtual worlds, but recommended:

i. building on existing regulations by targeting changes for the metaverse.
ii. dismantling regulations that hinder the development of the metaverse.
iii. involving all players in building the metaverse.

iv. building on existing standards and specifications and supporting the EU vision of virtual worlds within international frameworks; and
v. aiming for an open, interoperable, and interconnected metaverse ecosystem that can be accessed by anyone anywhere.

SMEunited also welcomed the Commission's envisaged initiative but stressed that it should take a risk-based and learning approach, as this would be balanced and not discouraging for SMEs. The association also highlighted that investing in developing such emerging technologies is necessary while ensuring a proper place for SMEs to develop virtual worlds.

(4) Academic/Research Institutions

GISMA University of Applied Sciences argued that legislative developments on this issue should follow the UNESCO's Recommendation on the Ethics of AI. They also stressed that the Commission should protect the privacy of users and ensure that operators of virtual worlds are held accountable for their actions.

AccessCat underscored the importance of virtual worlds' accessibility for all citizens through the inclusion of subtitles or audio subtitles.

(5) Other

Lastly, the International Association for Trusted Blockchain Applications (INATBA) stressed the importance of interoperability for the metaverse, but also emphasised that this should ensure the utmost safety and security. The organisation also noted that developers should devote more diligence and rigour to the code before launching any application.

The comments submitted to the public consultation are now expected to be considered by the Commission when finalising the measure.

Next steps

The comments submitted by stakeholders during the consultation are now expected to be taken into account by the Commission when finalising the expected non-legislative initiative, which is tentatively scheduled for adoption on 21 June 2023.

The Commission also convened a European Citizens' Panel on Virtual Worlds throughout the first quarter of 2023, which proposed 23 Recommendations for the development of fair and desirable virtual worlds in the EU. These Recommendations are also expected to be taken into account by the Commission.

Other Mechanisms

EU-US Privacy Shield

On 11 May the European Parliament adopted a Resolution urging the Commission not to move forward with its draft Implementing Decision (draft Adequacy Decision) regarding the EU-US Data Privacy Framework.

The European Parliament held a brief plenary debate to discuss the LIBE Committee's Report (draft Resolution) on the adequacy of the protection afforded by the EU-US Data Privacy Framework on 10 May 2023, then voted on and adopted the text in plenary as a Resolution (not yet publicly available) and consequently published a press release regarding the milestone on 11 May 2023.

On behalf of the Council, the Swedish Minister for EU Affairs stressed the importance of data flows for innovation and growth on both sides of the Atlantic. However, she also emphasised that such data sharing must be safe and in line with the GDPR and relevant CJEU decisions.

The Commissioner for Justice, Didier Reynders, then took the floor to note that the previous EU-US Privacy Shield had insufficient safeguards and allowed US intelligence agencies to obtain a lot of information on EU citizens.

However, the Commissioner underscored that the revised framework as outlined in the US Executive Order now follows the rights of the EU as stated by law and the courts. US intelligence agencies will now have to consider the necessity and proportionality requirements and a new redress mechanism has been established.

The Commissioner also stressed that the Commission would take action if any issues occur in the implementation of the framework.

Following this, the Rapporteur highlighted that the previous two frameworks were struck down by the CJEU and underlined that the proposed framework does not provide for sufficient safeguards. He therefore called upon the Commission to work on the remaining issues in order to prevent the measure from being struck down in the future. Several MEPs echoed the sentiments of the Rapporteur.

The following day, the European Parliament voted on the text and adopted it as a Resolution with 306 votes in favour, 27 against, and 231 abstentions, acknowledging that the proposed EU-US Data Privacy Framework is an improvement from previous frameworks, but stresses that it does not provide for sufficient safeguards to justify an adequacy decision on personal data transfers.

In particular, the Resolution points to the fact that the framework still allows for bulk collection of personal data in certain cases, does not make bulk data collection subject to independent prior authorisation, and does not provide for clear rules on data retention.

Additionally, the text criticises the proposed Data Protection Review Court (DPRC), which is aimed at providing redress to EU data subjects, as its decisions would be classified and not made public or available to complainants, violating citizens' right to access and rectify their data. The text also highlights that the DPRC would not be truly independent, as judges could be dismissed by the US President, who could also overrule its decisions.

Moreover, given that previous data transfer frameworks between the EU and the US were invalidated by rulings of the Court of Justice of the European Union (CJEU), the Resolution calls upon the Commission to ensure that the future framework will withstand legal challenges and provide legal certainty to EU citizens and businesses.

Therefore, the text urges the Commission not to grant an adequacy decision based on the current framework, as MEPs consider that the United States' level of personal data protection is not essentially equivalent to that of the EU. It also underscores that the Commission should instead negotiate a new 'future-proof' data transfer framework that is more likely to be held up in court.

Although the Resolution is non-binding, it may influence the Commission to reconsider its draft Adequacy Decision in part or in full.