TDL | Trust in Digital Life

European Proposals, Regulations and Initiatives 2023

May 2023

TDL | Trust in Digital Life

European Proposals, Regulations and Initiatives 2023

Table of contents

Proposals 3
- European Approach to Artificial Intelligence (AI Act) 4
- Cryptocurrencies 5
- Cyber Resilience Act 6
- Data Act 7
- European e-ID (eIDAS 2.0) 8
- e-Privacy 9
- EU Interoperability Framework 10
- Open Finance Framework 10

Regulations 12
- Digital Operational Resilience for Financial Sector (DORA) 13
- Digital Services Act (DSA) 13
- General Data Protection Regulation (GDPR) 14
- NIS Directive (Review) 14

Initiatives 19
- European Health Data Space 20
- Virtual Worlds (Metaverse) 21

Other Mechanisms 22
- EU-US Privacy Shield 23
- Digital Markets Act 24

TDL | Trust in Digital Life

Proposals

European Approach to Artificial Intelligence (AI Act)

Proposal

Laying down harmonised rules on artificial intelligence (also known as the AI Act)

Background

Following the presentation of its White Paper on AI, the Shaping Europe's Digital Future Communication, the Strategy for Data, as well as the 2030 Digital Compass initiative, the Commission presented a proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act).

Through this Regulation, the Commission intends to establish a legislative framework which would harmonise rules for placing on the market, or putting into use AI systems in the EU, as well as establishing certain requirements and prohibitions.

The Regulation would mainly apply to providers placing AI systems on the market and their users. It is worth highlighting that the Regulation would not apply to AI systems developed or used exclusively for military purposes.

An AI system would have to be understood as a software which is developed with one or more approaches or techniques (machine learning, logic- and knowledge-based approaches, statistical approaches) for a specific set of human-defined objectives, but can also generate outputs like content, predictions, recommendations or decisions influencing the environment they interact with.

Key Players

Commission

- Commissioner for Internal Market: Thierry Breton
- Executive Vice-President for a Europe Fit for the Digital Age: Margrethe Vestager

European Parliament Committees:

- The Internal Market and Consumer Protection (IMCO) - Joint Lead
- Civil Liberties Justice and Home Affairs (LIBE) - Joint Lead
- Industry, Research, and Energy (ITRE) - Associated
- Culture and Education (CULT) - Associated
- Legal Affairs (JURI) - Associated

Council

- Czech Presidency; French Presidency; Slovenian Presidency; Portuguese Presidency

TDL | Trust in Digital Life

Cryptocurrencies

Proposal

On Markets in Crypto-assets

Amending Directive (EU) 2019/1937

Background

The proposal covers crypto-assets that fall outside current digital finance legislation as well as e-money tokens and seeks to create a common legislative framework to prevent market fragmentation. It forms part of the Digital Finance Package presented by the Commission on 24 September 2020.

Key elements of the proposal include:

(1) Subject Matter, Scope and Definitions (Articles 1 to 3)

(2) Regulation of Crypto-Assets other than E-Money and Asset-Referenced Tokens (Articles 4 to 14)

(3) Regulation of Asset-Referenced Tokens (Articles 15 to 41):

- (A) Authorisation
- (B) Obligations
- (C) Acquisition
- (D) Definition of Significant Asset-Referenced Tokens

(4) Regulation of E-Money Tokens (Articles 43 to 52):

- (A) Authorisation
- (B) Definition of Significant E-Money Tokens

(5) Regulation of Crypto-Asset Service Providers (Articles 53 to 75):

- (A) Authorisation
- (B) Obligations
- (C) Acquisitions

(6) Preventing Crypto-Asset Market Abuse (Articles 76 to 80);

(7) Designation and Tasks of the Supervisory Authorities (Articles 81 to 120):

- (A) Powers of the national competent authorities,
- (B) Administrative sanctions,
- (C) EBA Supervisory Responsibilities and Powers.

The Digital Finance Package is composed of the following measures:

(a) the Digital Finance Strategy.

(b) a proposal for a Regulation on markets in crypto-assets.

(c) a proposal for a Regulation on the operational digital resilience of the financial sector.

(d) a proposal for a Regulation on a pilot regime for market infrastructures based on distributed ledger technology.

(e) a proposal for a Directive amending directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341; and

(f) the Retail Payments Strategy.

Key Players

Commission

- Commissioner for Financial services, financial stability and Capital Markets Union: Mairead McGuinness
- Executive Vice-President for an Economy that Works for People: Valdis Dombrovskis.

European Parliament

- Economic and Monetary Affairs (ECON)

European Council

- Portuguese Council Presidency, Slovenian Council Presidency, French Council Presidency, ECOFIN

Cyber Resilience Act

Proposal

On horizontal cybersecurity requirements for products with digital elements (also known as the Cyber Resilience Act (CRA))

Background

By way of this proposal for a Regulation, the Commission aims to introduce a legal framework to ensure the cybersecurity of digital products throughout their entire lifecycle to combat the rise in cyberattacks over the last few years.

The measure would also amend Annex I of Regulation (EU) 2019/1020, which establishes rules and procedures for economic operators and establishes a system for their cooperation with supervisory authorities in order to improve the functioning of the free movement of goods through the strengthening market surveillance of products covered by EU harmonisation legislation.

The proposal is closely connected to the 2020 Cybersecurity Strategy and builds on the Commission's Communication on Shaping Europe's Digital Future, as well as the Security Union Strategy. In addition, the proposal will complement the EU cybersecurity framework, which consists of the NIS Directive, the proposed NIS2 Directive, and the Cybersecurity Act.

Key Players

Commission

- Executive Vice-President for a Europe Fit for the Digital Age: Margrethe Vestager
- Vice-President for Promoting our European Way of Life: Margaritis Schinas
- Commissioner for the Internal Market: Thierry Breton

European Parliament Committees

- Industry, Research, and Energy (ITRE) - Lead
- The Internal Market and Consumer Protection (IMCO) - Associated
- Civil Liberties, Justice, and Home Affairs (LIBE) - Associated

Council

- Swedish Presidency; Czech Presidency
- Horizontal Working Party on Cyber Issues

Data Act

Proposal

Harmonised rules on fair access to and use of data

Background

By way of this proposal for a Regulation, the Commission aims to establish a horizontal framework for sharing non-personal data by introducing obligations that give users access to the data they contribute in generating and ensures that public bodies have access to privately-held data under exceptional circumstances.

The Data Act is the second main legislative initiative resulting from the European Strategy for Data and intends to complement the Data Governance Act, as well as the proposal for a Digital Markets Act. It also amends the Annexes of the Consumer Protection Regulation and the Injunctions Directive.

Rule 57 of the European Parliament's Rules of Procedure applies to this proposal. Under this rule, the ITRE (Lead) and JURI, 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.

The JURI and IMCO Committees adopted their respective Opinion and Opinion on 24 January 2023, while the LIBE Committee adopted its Opinion on 31 January 2023.

Key Players

Commission

- Commissioner for Internal Market: Thierry Breton
- Executive Vice-President for a Europe Fit for the Digital Age: Margrethe Vestager

European Parliament Committees

- Industry, Research, and Energy (ITRE) - Lead
- Legal Affairs (JURI) - Associated
- Civil Liberties, Justice, and Home Affairs (LIBE) - Associated

Council

- Swedish Presidency; Czech Presidency; French Presidency
- Working Party on Telecommunications and Information Society

European e-ID (eIDAS 2.0)

Proposal

Establishing a framework for a European Digital Identity (also known as eIDAS 2.0)

Background

The proposal was first announced in the Commission's Letter of Intent in the State of the Union on 16 September 2020. It builds upon Regulation (EU) No 910/2014, which lays down the conditions under which the Member States recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State.

The Commission presented the proposal on 3 June 2021.

Rule 57 of the European Parliament's Rules of Procedure applies to the proposal. Under this rule, the ITRE (Lead), as well as the IMCO, JURI, 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.

The IMCO Committee adopted its Opinion on 12 September 2022, while the LIBE Committee adopted its Opinion on 10 October 2022. The JURI Committee then adopted its Opinion on 27 October 2022.

Key Players

Commission

- Commissioner for Internal Market: Thierry Breton
- Executive Vice-President for a Europe Fit for the Digital Age: Margrethe Vestager

European Parliament Committees

- Industry, Research and Energy (ITRE) - Lead
- Internal Market and Consumer Protection (IMCO) - Associated
- Legal Affairs (JURI) - Associated
- Civil Liberties Justice and Home Affairs (LIBE) - Associated

Council

- Swedish Presidency; Czech Presidency; French Presidency; Slovenian Presidency; Portuguese Presidency

e-Privacy

Proposal

Concerning the respect for private life and the protection of personal data in electronic communications

Background

The Commission presented its proposal for a Regulation on 10 January 2017, that would revise and repeal the current e-privacy Directive 2002/58/EC.

The e-Privacy Directive complements the current Data Protection Directive 95/46/EC revised by the General Data Protection Regulation which sets out general principles with regard to the processing of personal data, in order to ensure the free flow of information on the one hand and the rights and freedoms of natural persons on the other.

Key Players

Commission

- Commissioner for the Internal Market - Thierry Breton

European Parliament Committees

- Civil Liberties, Justice, and Home Affairs Committee (LIBE)

Council

- Swedish Presidency; Czech Presidency; French Presidency; Slovenian Presidency, Portuguese Presidency, German Presidency, Croatian Presidency, Finnish Presidency, Romanian Presidency.

EU Interoperability Framework

Proposal

Laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act)

Background

The 2022 Commission Work Programme announced the Commission's ambition of increasing interoperability and cross-border cooperation of public administrations. With this in mind, the Commission announced its intention to present a proposal to increase interoperability among EU governments and public administrations.

The proposal will seek to lay down a new legal framework for interoperability for EU governments to coordinate efforts and implement common standards for secure public sector data flows and services across borders.

This builds upon the European Interoperability Framework, a non-binding implementation strategy that provided guidance to administrative entities to electronically exchange, among themselves and with citizens and businesses, information in ways that are understood by all parties.

Key Players

Commission

- Commissioner for Internal Market: Thierry Breton
- Executive Vice-President for a Europe Fit for the Digital Age: Margrethe Vestager

European Parliament Committees

- Industry, Research and Energy (ITRE)
- Civil Liberties, Justice, and Home Affairs (LIBE) - Associated

Council

- Swedish Presidency; Czech Presidency
- Working Party on Telecommunications and Information Society

Open Finance Framework

Background

The expected proposal would help the financial services sector have better financial products, better targeted advice, improved access for consumers and greater efficiency in business-to-business transactions.

The measure was announced in the Digital Finance Strategy presented by the Commission on 24 September 2020.

The Digital Finance Strategy sets out a strategic objective for digital finance in Europe, and four priorities and related actions that the Commission intends to take to enable consumers and businesses to enjoy the benefits of digital finance while also mitigating risks.

Key Players

Commission

- Commissioner for Financial services, financial stability and Capital Markets Union: Mairead McGuinness
- Executive Vice-President for an Economy that Works for People: Valdis Dombrovskis.

TDL | Trust in Digital Life

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 and applies from 17 January 2025.

Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

Background

The Regulation is part of the Digital Finance Package presented by the Commission on 24 September 2020, which also included:

(a) the Digital Finance Strategy

(b) a proposal for a Regulation on markets in crypto-assets

(c) a proposal for a Regulation on a pilot regime for market infrastructures based on distributed ledger technology

(d) a proposal for a Directive amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341; and

(e) the Retail Payments Strategy.

Digital Services Act (DSA)

Regulation

On a Single Market For Digital Services

Background

The Commission proposed the Digital Services Act (DSA) together with the Digital Markets Act (DMA) on 15 December 2020 to update the horizontal regulatory framework for digital services in the Single Market.

The DSA focuses on upgrading the liability and safety rules for digital platforms, services, and products, whereas the DMA introduces rules for platforms that act as "gatekeepers" in the digital sector and aims to prevent them from imposing unfair conditions on businesses and consumers.

Key Players

Commission

- Executive Vice-President for a Europe Fit for the Digital Age: Margrethe Vestager
- Vice-President for Values and Transparency: Věra Jourová
- Commissioner for Justice: Didier Reynders
- Commissioner for Internal Market: Thierry Breton

European Parliament Committees

- Committee on Internal Market and Consumer Protection (IMCO) - Lead Committee
- Industry, Research and Energy Committee (ITRE) - Associated Committee
- Civil Liberties, Justice and Home Affairs Committee (LIBE) - Associated Committee
- Legal Affairs Committee (JURI) - Associated Committee

Council

- Czech Presidency; French Presidency, Slovenian Presidency; Portuguese Presidency; German Presidency

General Data Protection Regulation (GDPR)

Regulation (EU) 2016/679 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

Replaces

Directive 95/46/EC

Background

The European Data Protection Board (EDPB) is an independent body with a legal personality, responsible for ensuring the consistent application of the (GDPR).

It succeeded the Article 29 Working party, and it is composed of the Member States data protection authorities and the EDPS.

Key Players

Members of the EDPB - representatives of the national data protection authorities.

NIS Directive (Review)

Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) entered into force on 16 January 2023, following its publication in the EU Official Journal on 27 December 2022.

The Directive is divided into nine chapters and contains the following key elements:

Chapter I - General Provisions (Articles 1-6)

The general aim of the Directive is specified in Article 1 as to achieve a high common level of cybersecurity across the Union. To this end, the Directive lays down measures to require Member States to adopt national cybersecurity strategies and designate competent cyber crisis management

authorities, rules and obligations on cybersecurity information sharing, and supervisory and enforcement obligations.

Article 2 delineates the scope of the Directive to cover public or private entities that qualify as or exceed medium-sized enterprises which provide their services or carry out their activities within the EU.

However, the Directive does not apply to public administration entities in the areas of national security, public security, defence or law enforcement, or entities exempted from the scope of Regulation (EU) 2022/2554 (DORA).

Article 3 lays down the criteria for essential and important entities and outlines the obligations of Member States regarding such entities.

Moreover, Articles 4 and 5 enshrine the primacy of specific-sector Union legal acts over the Directive, and the minimum harmonisation principle, respectively. Article 6 offers a list of definitions used throughout the text.

Chapter II - Coordinated Cybersecurity Frameworks (Articles 7-13)

Article 7 lays down the minimum requirements for the national cybersecurity strategies that Member States are required to adopt, including strategic objectives, resources required to achieve those objectives, and appropriate regulatory measures.

Articles 8 and 9 deal with the designation of a competent authority and single contact point in each Member State and their responsibility for the management of large-scale cybersecurity incidents and crises.

Article 10 establishes computer security incident response teams (CSIRTs) in each Member State, which are to be responsible for incident handling and cooperation with other national and international bodies.

Subsequently, Article 11 lists certain requirements for the CSIRTs and their tasks, such as monitoring and analysing cyber threats, providing early warnings, responding to incidents, or collecting and analysing forensic data, among others.

Article 12 obliges Member States to designate one of its CSIRTs as a coordinator for the purposes of coordinated vulnerability disclosure. Its tasks would include identifying and contacting the entities concerned, assisting the persons reporting a vulnerability, negotiating disclosure timelines, and managing vulnerabilities that affect multiple entities.

Furthermore, Article 13 concerns the cooperation of different competent authorities at the national level.

Chapter III - Cooperation at Union and International Level (Articles 14-19)

Article 14 creates a Cooperation Group to facilitate strategic cooperation and the exchange of information among Member States. Its tasks include providing guidance to the competent authorities, facilitating the exchange of best practices and information, carrying out coordinated security risk assessments of critical supply chains, and organising meetings with relevant private stakeholders from across the Union, among others.

In addition, Article 15 establishes a network of national CSIRTs to facilitate the sharing, transfer, and exchange of technology and relevant measures among the CSIRTs, ensuring the interoperability of protocols, and discussing and identifying further forms of operational cooperation, among others.

Article 16 establishes the European cyber crisis liaison organisation network (EU-CyCLONe), responsible for increasing the level of preparedness of the management of large-scale cybersecurity incidents and crises, developing a shared situational awareness of cyber crises, and reporting on a regular basis to the Cooperation Group on the management of incidents, among others.

Article 17 enables the EU to conclude international agreements with countries or international organisations, while Article 18 requires EINSA to adopt a biennial report on the state of cybersecurity in the Union.

Moreover, Article 19 obliges the Coordination Group to establish the methodology and organisational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Member States' cybersecurity capabilities and policies necessary to implement this Directive.

Chapter IV - Cybersecurity Risk-Management Measures and Reporting Obligations (Articles 20-25)

Article 20 specifies the governance structure, while Article 21 lays down specific cybersecurity risk-management measures to be ensured by Member States.

Furthermore, Article 22 regulates the coordinated security risk assessments to be carried out by the Cooperation Group, and Article 23 lays down the reporting obligations of Member States.

Article 24 allows Member States to require essential and important entities to use particular ICT products, services, and processes certified under European cybersecurity certification schemes. The Commission is empowered to adopt delegated acts in this regard.

Article 25 encourages Member States to promote the use of European and international standards relevant to the security of network and information systems.

Chapter V - Jurisdiction and Registration (Articles 26-28)

Article 26 establishes that entities under the scope of the Directive are considered to fall under the jurisdiction of the Member State in which they are established, with the exception of: (a) providers of public electronic communications networks; (b) entities such as DNS service providers and TLD name registries, among others; and (c) public administration entities.

Article 27 obliges ENISA to create and maintain a registry of DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, as well as providers of online marketplaces, of online search engines and of social networking services platforms.

Article 28 mandates Member States to require TLD name registries and entities providing domain name registration services to collect and maintain a domain name registration data in a dedicated database with some minimum data such as the domain name, the registrant's name, or their contact information.

Chapter VI - Information Sharing (Articles 29-30)

Article 29 regulates cybersecurity information-sharing arrangements between entities falling within the scope of this Directive and other entities outside of the scope. In addition, the exchange of information within communities of essential and important entities, and between them and the Member States, is also encouraged.

Article 30 enables any entity, essential and important or not, to submit a notification to CSIRTs with regard to incidents, cyber threats, and near misses.

Chapter VII - Supervision and Enforcement (Articles 31-37)

Articles 31 and 32 require Member States to ensure that their competent authorities effectively supervise and comply with the Directive in an effective and proportionate manner.

Furthermore, Article 33 sets out the supervisory and enforcement measures in relation to important entities, while Article 34 lays down the general conditions for imposing administrative fines on essential and important entities.

Infringements entailing personal data breach are outlined in Article 35 and penalties are laid down in Article 36. Moreover, Article 37 promotes mutual assistance between competent authorities of different Member States.

Chapter VIII - Delegated and Implementing Acts (Articles 38-39)

Article 38 confers the Commission with powers to adopt delegated acts, while Article 39 allows for the Commission to be assisted by a committee.

Chapter IX - Final Provisions (Articles 40-46)

Pursuant to Article 40, the Commission will be required to submit to the European Parliament and to the Council a report assessing the functioning of this Directive.

Furthermore, Article 41 states that Member States must transpose the Directive by 17 October 2024.

Lastly, Articles 42 and 43 amend Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, respectively, while Article 44 repeals Directive (EU) 2016/1148 with effect from 18 October 2024.

The Directive is followed by three Annexes, which outline: (i) the sectors of high criticality; (ii) other critical sectors; and (iii) a correlation table.

Background

The proposal followed the ordinary legislative procedure under the Lisbon Treaty.

In line with the Commission's 'Cybersecurity Strategy' and the Communication 'Shaping Europe's Digital Future' and also with the rise of cybersecurity threats originating outside of the EU, the Commission presented on 16 December 2020 its proposal on measures for a high common level of cybersecurity across the Union.

The Directive will repeal Directive (EU) 2016/1148 on 18 October 2024, which establishes measures to ensure a high common level of network and information security across the Union.

Key Players

Commission

- Commissioner for Internal Market: Thierry Breton
- Executive Vice-President for a Europe Fit for the Digital Age: Margrethe Vestager

European Parliament Committees

- Industry, Research and Energy (ITRE) - Lead
- Civil Liberties, Justice and Home Affairs (LIBE) - Associated

Council

- Czech Presidency; French Presidency; Slovenian Presidency; Portuguese Presidency

TDL | Trust in Digital Life

Initiatives

European Health Data Space

The initiative focuses on promoting health data exchange across the EU and supporting health research, particularly on new preventative strategies but also on treatments, medicines, medical devices and outcomes, and tackling barriers to the cross-border division of digital health services and products.

The initiative would also facilitate the establishment of a Code of Conduct for processing personal data in the health sector, in accordance with Article 40 of the General Data Protection Regulation.

Notably, the proposal builds upon the proposed Data Governance Act and the proposed Data Act, NIS Directive (under revision), a proposal for a Cyber Resilience Act, the Medical Devices Regulation, In Vitro Diagnostics Regulation, General Data Protection Regulation and others.

In addition, the EHDS aims at addressing the shortcomings of the Directive 2011/24/EU on the application of patients' rights in cross-border healthcare, which had a rather limited impact on supporting natural persons' access to and control over their electronic health data.

The creation of an EU Health Data Space is part of the Commission's agenda for digital transformation, which was announced in February 2020 in the Communication on Shaping Europe's Digital Future, the Communication on a European Strategy for Data, and the White Paper Artificial Intelligence.

Key Players

- Commissioner for Internal Market: Thierry Breton
- Executive Vice-President for a Europe Fit for the Digital Age: Margrethe Vestager
- Commissioner for Health and Food Safety: Stella Kyriakides

European Parliament Committees

- Civil Liberties, Justice and Home Affairs (LIBE)
- The Environment, Public Health and Food Safety (ENVI)
- Internal Market and Consumer Protection (IMCO) (Associated)
- Industry, Research and Energy (ITRE) (Associated)

Council

- German Presidency / Portuguese Presidency / Slovenian Presidency / Czech Presidency / Swedish Presidency

Other bodies

- General Data Protection Board
- eHealth Network

External contractor

- EUHealthSupport consortium

Stakeholders

- European Federation of Nurses Associations
- The League of European Research Universities

- European Health Data & Evidence Network
- European Association of E-Pharmacies
- German Chemical Industry Association
- Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (ZVEI)
- EuroHealthNet
- Sanofi
- Dachverband der Österreichischen Sozialversicherungen
- Philips
- European Association of Hospital Pharmacists
- ACT | The App Association
- Microsoft
- European Cancer Patient Coalition
- European Hospital and Healthcare Federation (HOPE)
- Association of Clinical Research Organizations (ACRO)
- Pharmaceutical Group of the EU (PGEU)
- European Patients' Forum (EPF)
- European Public Health Alliance

Virtual Worlds (Metaverse)

The expected non-legislative initiative on virtual worlds such as the metaverse was first announced in the Commission's 2022 Letter of Intent on 14 September 2022.

While many stakeholders have welcomed a general vision for the expected non-legislative initiative on virtual worlds, several recommendations were offered.

The metaverse, the literal meaning of which translates to 'beyond universe', is generally known to be an immersive and constant virtual 3D world where people interact through the use of avatars to do things such as enjoy entertainment, make purchases, and work without physically leaving their seat.

According to a statement published by the Commissioner for the Internal Market, Thierry Breton, the European vision to foster virtual worlds will include three crucial aspects: putting people at the centre, developing cutting-edge technologies, and building a resilient infrastructure.

Prior to its adoption, the Commission convened a European Citizens' Panel on Virtual Worlds, the objective of which was to formulate a set of guiding principles and actions for the development of such worlds in the EU.

The Panel met three times. The first session took place on 24-26 February 2023 and consisted of participants building a shared vision of what desirable and fair virtual worlds should look like with the support of external speakers.

The second session took place on 10-12 March 2023 and had participants identify, discuss, and prioritise values and principles that they considered should guide the development of virtual worlds in the EU.

The third and final session took place on 21-23 April 2023 and had participants turn their ideas into concrete Recommendations and develop a catalogue of preferred actions towards the development of desirable virtual worlds.

Key Players

Commission

- Executive Vice-President for a Europe Fit for the Digital Age: Margrethe Vestager
- Commissioner for the Internal Market: Thierry Breton

Other Mechanisms

EU-US Privacy Shield

The European Union and the United States conducted negotiations for a renewed transatlantic data transfer framework (also known as the Privacy Shield) and reached a political agreement 'in principle' on 25 March 2022.

The U.S. Government and the European Commission then had to translate the arrangement into legal documents. On the US side, these commitments were outlined in an Executive Order, which was signed by the President of the United States of America, Joe Biden, on 7 October 2022.

Following the publication of the Executive Order, the Commission presented a draft Implementing Decision (Adequacy Decision) on the adequacy of the protection provided by the new transatlantic data privacy framework on 12 December 2022, in accordance with Article 45 of Regulation (EU) 2016/679(the GDPR).

The draft Implementing Decision follows the "examination procedure" for "implementing acts" under the Lisbon Treaty.

Following its presentation, the draft measure was sent to the European Data Protection Board (EDPB), which issued an Opinion on 28 February 2023.

The draft measure will also be presented to the Committee on the protection of individuals with regard to the processing of personal data and on the free movement of such data (also known as the Article 93 Committee), which is composed of Member State experts, for an Opinion following a vote. The Committee would deliver its opinion via qualified majority.

If the Committee gives a favourable Opinion, or if it fails to reach an Opinion by a qualified majority, then the Commission may adopt the draft measure.

Once this procedure is complete, the Implementing Decision may then be published in the EU Official Journal and enter into force.

In parallel, the European Parliament has a right of scrutiny over Adequacy Decisions, and it adopted a Resolution (not yet publicly available) on the EU-US Data Privacy Framework on 11 May 2023.

The Resolution urges the Commission not to adopt its draft Adequacy Decision, as the Parliament considers that the Framework fails to create actual equivalence in the level of protection. Although non-binding, the Resolution may influence the Commission to reconsider its draft Adequacy Decision in part or in full.

Background

The original EU-US Privacy Shield was a mechanism established by Commission Implementing Decision (EU) 2016/1250 on 12 July 2016, which allowed for the free transfer of personal data from EU companies to US companies certified under the Shield.

This Decision replaced Decision 2000/520/EU, which recognised the Safe Harbour international privacy principles issued by the U.S. Department of Commerce as providing adequate protection for the purposes of personal data transfers from the EU to organisations established in the United States.

However, the European Court of Justice (ECJ) struck down both mechanisms and created a vacuum in this area: the Privacy Shield was repealed on 16 July 2020 by the Schrems II ruling, whereas the Safe Harbour mechanism was invalidated by the ECJ on 6 October 2015.

Following these decisions, the Commission and the US Government commenced negotiations in August 2020 to find a successor arrangement and evaluate the potential for an enhanced EU-U.S. Privacy Shield framework to comply with the judgement of the Court in the Schrems II case.

Key Players

European Union

- President of the European Commission: Ursula von der Leyen
- Commissioner for Justice: Didier Reynders

United States of America

- US President: Joseph R. Biden
- US Secretary of Commerce: Gina Raimondo

European Parliament Committee

- Civil Liberties, Justice, and Home Affairs (LIBE)

Digital Markets Act

Regulation

On contestable and fair markets in the digital sector

Amending Directives (EU) 2019/1937 and (EU) 2020/1828