# Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect their Victims

**H2020 – 101021801**

www.heroes-fct.eu

# D3.6 Final HEROES data protection legal framework

**Authors**

Sara Domingo Andrés

Ben Howkins

| | |
|---|---|
| Deliverable nature | Report (R) |
| Dissemination level | Public (PU) |
| Version | 1.0 |
| Date | 29/12/2023 |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021801

# Document Information

| | |
|---|---|
| **Project Acronym** | HEROES |
| **Project Title** | Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect their Victims – HEROES |
| **Grant Agreement No.** | 101021801 |
| **Project URL** | www.heroes-fct.eu |
| **EU Project Officer** | Elina Manova |

| | | | | | |
|---|---|---|---|---|---|
| **Deliverable** | **Number** | D3.6 | **Title** | Final HEROES Data Protection Legal Framework | |
| **Work Package** | **Number** | WP3 | **Title** | Privacy, ethical data management and social impact assessment | |
| **Date of Delivery** | **Contractual** | | M24 | **Actual** | M24 |
| **Status** | Version 1.0 | | | Final | |
| **Nature** | R | | **Dissemination level** | | PU |

| | | | | |
|---|---|---|---|---|
| **Responsible partner** | **Name** | Sara Domingo Andres | **E-mail** | Sara.domingo.andres@trilateralresearch.com |
| | **Partner** | TRI | **Phone** | +353 (0)51 833 958 |
| **Contributing partners** | N/A | | | |
| **Reviewers** | Juan Carlos Ortiz Pradillo (UCM), Gemma Galdon Clavel (External Ethics Advisor and Chief of the EAB) | | | |
| **Security Approval** | Julio Hernandez-Castro (UNIKENT) | | | |

**Abstract (for dissemination)**
As a second iteration of D3.3, this D3.6 aims at providing an overview of the legislative developments and policy trends in the EU that will have an impact on the tools that are being researched and developed within the HEROES project.

| | |
|---|---|
| **Keywords** | E-evidence, AI Act, DSA, legislative developments and policy trends |



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021801. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

# Version History

| Version | Date | Change Editor | Changes |
|---|---|---|---|
| 0.1 | 20/11/23 | Sara Domingo Andres (TRI)<br>Ben Tomkins (TRI) | Drafting V1 |
| 0.2 | 23/11/23 | Zachary Goldberg (internal review) | Introduction, conclusion, proofreading |
| 0.3 | 23/11/23 | Christopher Nathan (TRI internal review) | Introduction, conclusion, proofreading |
| 0.4 | 23/11/23 | Agnel Nidhi Shiji | Introduction, conclusion, proofreading |
| 0.5 | 7/12/2023 | Gemma Galdon Clavel (EAB) | Review and comments |
| 0.6 | 12/12/2023 | Juan Carlos Ortiz Pradillo (UCM) | Review and comments |
| 0.7 | 28/12/2023 | Julio Hernandez-Castro (UNIKENT) | SAB review |
| 1.0 | 29/12/2023 | Luis Javier García Villalba (UCM) | Final review for submission |

# Table of Contents



 

# Executive summary

This deliverable analyses the legal and policy developments in the EU, and internationally, that affect the exchange of e-evidence for law enforcement purposes, the management and processing of data by network operators, and the development and deployment of AI tools to combat CSA/E and THB. The deliverable categorises the relevant laws and proposals into three groups: those affecting network operators, those affecting LEAs, and those affecting technical partners. The deliverable also highlights the main issues and challenges that arise from these laws and proposals, such as the protection of privacy and personal data, the protection of minors, the balance between security and human rights, and the compliance and exploitation of the HEROES tools. Some of the key points from the deliverable are:

- The Digital Services Act (DSA) and the Online Safety Act (OSA) introduce a new regime for the policing of CSAM, requiring network operators to report such content to LEAs and imposing other obligations and safeguards.

- The e-Privacy Regulation is a proposed EU law that will protect privacy and personal data in electronic communications, applying to all service providers and end-users in the EU and regulating various aspects of electronic communications.

- The UK Online Safety Act (OSA) aims to make internet services safer, especially for children, by imposing duties on providers to prevent harm from illegal and harmful content, while maintaining privacy standards. However, the OSA may also enable mass surveillance of all digital communications by firms in the private sector, creating tensions between its different objectives.

- The e-evidence package is a set of EU laws that aim to simplify the cross-border access to e-evidence for law enforcement purposes but may also raise privacy and data protection issues. The e-evidence package also covers the cooperation between the EU and third countries, especially the US, on e-evidence matters.

- The AI Act is a proposed EU law that aims to regulate AI in a way that ensures trustworthiness, ethics, and human-centricity, while fostering innovation and competitiveness in the EU. The AI Act also establishes a risk-based approach to AI regulation, with different rules and requirements for different categories of AI systems. It also envisages the role of standards and conformity assessment bodies in ensuring the compliance of AI systems with the legal framework.

We conclude noting that while there is a great deal of legislative activity in these fields, there are also reasons to expect a degree of uncertainty about the nature of the developing regime for some time to come.

# Abbreviations

| | |
|---|---|
| AI | Artificial Intelligence |
| CJEU | Court of Justice of the European Union |
| CSA | Child Sexual Abuse |
| CSA/E | Child Sexual Abuse and Exploitation |
| CSAM | Child Sexual Abuse Material |
| DSA | The Digital Services Act Regulation (the "DSA") (Regulation 2022/2065) |
| EC | European Commission |
| EP | European Parliament |
| EU | European Union |
| EDPS | European Data Protection Supervisor |
| GDPR | General Data Protection Regulation 2016/679 |
| ISO | International Organisation for Standardisation |
| ISP | Internet Service Provider |
| LEA(s) | Law Enforcement Authority(ies) |
| LED | Law Enforcement Directive (2016/680) |
| OSB | Online Safety Bill (UK) |
| OSA | Online Safety Act (UK) |
| SIENA | Secure Information Exchange Network Application |
| THB | Trafficking in Human Beings |
| UK | United Kingdom |

# Definitions

| | |
|---|---|
| **DSA** | The Digital Services Act, EU Regulation 2022/2065. |
| **E-evidence** | Digital data that is used to investigate and prosecute criminal offences. |
| **E-evidence Regulation** | Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. |
| **E-evidence Directive** | Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. |
| **E-Privacy Directive** | Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications). |
| **E-Privacy Regulation** | Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), 2017/0003. |
| **GDPR** | Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). |
| **OSB** | UK Online Safety Bill (285) / Act 2023 |
| **Umbrella Agreement** | EU-US Data Protection and Privacy Agreement, 2016. |
| **Recommendation** | Council of the EU, Feb 2019, Recommendation for a COUNCIL DECISION authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters |
| **UK – US Agreement** | The UK-US Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [CS USA No.6/2019]. |
| **Australia – US Cloud Agreement** | Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime. |

# 1. Introduction

As a second iteration of deliverable 3.3, this deliverable will continue to explore and analyse legislative proposals, developments, policies and recent approvals in Europe and the United States that will have a direct impact on: (1) how Law Enforcement Authorities ("**LEAs**") carry investigations and gather electronic data and evidence in cases where there is a cross-border element, within the EU boundaries or beyond; (2) how data is managed and processed by network operators that ultimately will have an impact on the information exchange with LEAs; and (3) regulations that will be binding for developers of technological tools to combat child sexual abuse ("**CSA**") and child sexual abuse material ("**CSAM**") and trafficking in human beings ("**THB**") .

In addition to the cross-border gathering of electronic evidence ("**e-evidence**"), there are several regulations that will directly impact the development and deployment of the HEROES tools, such as, the proposals for an Artificial Intelligence Act, an E-privacy Regulation, and the UK online safety bill, along with recently approved laws including the e-evidence package, the Directive on the exchange of information between LEAs and the new framework to combat CSAM.

Given the variety of laws and proposals at an EU and non-EU level, we have grouped them in 3 different categories: (1) laws affecting network operators (providers of online services such as, social networks and instant messaging services); (2) laws affecting LEAs; and (3) laws affecting technical partners. It should be noted that the classification in three groups has been carried out for mere organisational purposes; and as such, laws classified in the first group will have a direct impact on network operators but will also indirectly affect LEAs since these laws defined what data network operators should collect and for what purposes and therefore LEAs might be in a position to request these data. In the same way, laws listed in the second group will directly affect LEAs but also network operators since they will govern how e-evidence is requested; and lastly the third group will contain laws affecting technical partners but also LEAs. In this regard, technical partners will need to develop their tools in accordance with the Artificial Intelligence Act ("AI Act") but LEAs serving as end-users of the AI tools will also need to abide by its provisions.

The deliverable explores legislative changes that will not only impact technical partners in the HEROES project in their work delivering tools to LEAs, but will also directly affect LEAs in their exercise of their duties to identify, prevent and prosecute CSAM and THB in the online world. Furthermore, it is of immediate relevance to how LEAs will interact with ISPs in the future, especially under the new Online Safety Act in the UK.

Further key points from the deliverable are as follows:

- The Digital Services Act and the Online Safety Act present a novel regime in the policing of CSAM. Before, the approach centred on voluntary reporting. In the new legislative environment service providers are mandated to report to LEAs.
- The e-Privacy Regulation is a proposed EU law to protect privacy and personal data in electronic communications. It will apply to all service providers and end-users in the EU. It will also regulate direct marketing, metadata and terminal equipment.
- The UK Online Safety Act (OSA) aims to make internet services safer, especially for children, by imposing duties on providers to prevent harm from illegal content, while maintaining privacy standards. Depending on how it is implemented, the Act's various aims may be brought into conflict as a result of a potentially far-reaching clause that may mandate mass surveillance of all digital communications by firms in the private sector.
- E-evidence is digital data held by online service providers that can help prosecute crimes. However, accessing it across jurisdictions is difficult and slow. The EU's e-evidence package aims to simplify

 

the process but may raise privacy and data protection issues. The US-EU cooperation on e-evidence is also explored, as well other elements of international cooperation, including the issue of reciprocity.

- The EU's proposal to regulate AI in the form of the AI Act is still under negotiation and may affect the HEROES tools' compliance and exploitation. The text updates the HEROES partners on the latest developments and obligations, including the draft Act's concept of a 'high risk' AI; the need for and nature of fundamental rights impact assessments; and the delegation of key implications of the Act to standards development.

# 2. Legislative developments for network operators

## 2.1. The e-Privacy Regulation

### 2.1.1. Introduction

In 2017, the EC published its proposal for a "Regulation concerning the respect for private life and the protection of personal data in electronic communications" (the "**e-Privacy Regulation'**)[1] which is meant to repeal Directive 2002/58 (the "**e-Privacy Directive**").

Initially, the e-Privacy Regulation was intended to come into force at the same time as the General Data Protection Regulation 2016/679 (the "**GDPR**") that is in May 2018, however, the e-Privacy Regulation legislative process has been delayed significantly ever since it was proposed. The Council's amendments and new draft proposal was published in February 2021[2] which contains significant amendments from the original proposal. This new draft proposal is now being discussed amongst the EC, the EP and the Council (trilogue negotiations) but there is not an estimated date of approval or inter-institutional agreement. The following sections have been written following the Council's text.

The aim of the Regulation is to achieve a higher level of harmonisation around the rules for the protection of privacy and personal data processed in electronic communications, which currently are being governed by a Directive that is considered to be outdated since it entered into force in 2002 and which required national transposition leaving certain aspects to the discretion of Member States and its regulation through national laws. In addition, the e-Privacy Regulation will be '*lex specialis*'[3] to the GDPR, meaning that if there is a conflict between the provisions of the GDPR and the e-Privacy Regulation for an activity or situation within the realm of the e-Privacy Regulation, the latter will prevail.

### 2.1.2. Material and territorial scope

Pursuant to Articles 2 and 3 of the proposal, the Regulation will apply to the provision and use of electronic communications services to end-users irrespective of whether a payment for such services is required and the protection of information related to the terminal equipment of end-users. When referring to electronic communications the proposal includes its content and metadata (Article 2.1.a). It also regulates the sending of direct marketing communications and the offering of publicly available directories. Similarly, to the regime introduced by the GDPR, the Regulation will apply to service providers rendering its services to end-users in the EU whether they are established in the EU or not. If service providers are not established in the EU, they shall designate a representative.

### 2.1.3. Key elements of the e-Privacy Regulation

The proposal will specifically apply to the so-called over-the-top services (OTT) such as WhatsApp, Facebook Messenger and Skype. One of its novelties is that it contains strict rules that do not only oblige service providers to guarantee the confidentiality of the content of the electronic communications but also its related metadata. This reference to metadata is new in data protection law which is defined in Article 4 as "*data processed by means of electronic communications services for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication*".

[1] E-Privacy Regulation Proposal: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010
[2] Council of the EU, February 2021, amendments and new text draft: https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf
[3] Context of the e-Privacy Regulation Proposal, point 1.2: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010

 

Similarly, to the e-Privacy Directive, and honouring Article 8.2 of the European Convention on Human Rights, Article 5 provides that electronic communications shall be confidential and any interference "*including, listening, tapping, soring, monitoring, scanning or other kinds of interception, surveillance and processing […] by anyone other than the end-users concerned, shall be prohibited, except when permitted by this Regulation*". Any other interference carried out for the sake of law enforcement would not fall within the scope of the e-Privacy Regulation as specified in Article 2.2 (d).

Article 6 outlines the exceptions to the general rule of no interference and exhaustively lists the instances where communications data, content and metadata could be processed by network operators. Amongst others, processing that is necessary to provide the services and maintain its security; processing that it is necessary to comply with a legal obligation, and remarkably where end-user has given consent.

The necessity to obtain consent is not new to the e-Privacy Regulation; it was already provided in Article 5 of the e-Privacy Directive. However, the proposal has given rise to what some call the most lobbied regulation in history, because it will provide stricter rules to the consent applicable to cookies where users shall be allowed when visiting a website to choose only the use of necessary or functional cookies. In addition, stricter rules for consent will apply to marketing communications and blocking unwanted, malicious or nuisance calls.

## 2.2. The DSA and the interim and proposed regulations to combat CSA

As referred in D3.2, the Digital Services Act (the "**DSA**") (Regulation 2022/2065), came into force in November 2022 and shall apply from the 17th of February 2024. The Act creates new obligations for internet service providers: social network operators, content sharing platforms, app stores, etc, to act on illegal content, listing explicitly CSAM. In this line, internet service providers will have the legal obligation to:

- implement measures to counter illegal goods, services or content online, including CSAM, such as a mechanism for users to flag such content and for platforms to cooperate with "trusted flaggers". Recital 61 points at the INHOPE network of hotlines for reporting CSAM as an example of trusted flagger.
- carry out risk assessments considering foreseeable negative effects for the rights of the child enshrined in the Charter of Fundamental Rights of the EU, this obligation is only applicable to providers of very large online platforms.
- implement mitigation measures to protect the rights of the child including age verification and parental control tools aimed at helping minors signal abuse or obtain support, applicable to providers of very large online platforms.

Nonetheless, internet service providers and network operators are and will be bound by the provisions on the new framework to combat CSAM online which are *lex specialis* to the DSA, i.e., the interim Regulation[4] and the proposed regulation to prevent and combat CSA that will eventually replace the interim Regulation[5]. Therefore, while the DSA governs addressing illegal content online in general, the proposed regulation to combat CSAM will introduce more specific rules for child protection.

The DSA and the interim and proposed regulations to combat CSA entail a paradigm shift from the early days of internet policy and regulations when internet service providers had no obligations to proactively identify illegal and harmful content within their own realms of activity. This new regime has been introduced as a consequence of the rising and increasing CSAM content shared online within the last few years (further information around this can be found in D3.2). Nonetheless, it has also been received with a certain level of

[4] Regulation 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the pu rpose of combating online child sexual abuse: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R1232

[5] Regulation laying down rules to prevent and combat child sexual abuse' (2022/0155(COD)) (2022): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN

controversy and has sparked criticism on the grounds of surveillance since it will oblige internet service providers to scan user communications and activities to some extent in order to proactively identify and report CSAM.

Further information around the rules contained in the interim regulation and the proposed regulation to combat CSA can be found in D3.2 of the HEROES project. As of today (November 2023), the proposal is still being negotiated and the Council is still having internal discussions, including with its preparatory bodies, but neither the Council or the European Parliament have agreed on their official positions. In October 2023, EURACTIV[6] and other media published that members of the European Parliament have reached an agreement on the draft law, restricting the obligations of service providers to monitor, identify and report CSAM in private chats amid surveillance accusations. By contrast, some of the media have claimed that the new draft would empower judicial authorities to request service providers to scan such content only where there is reasonable suspicion that an individual or group is linked to CSAM[7]. It is argued that this way, end-to-end encryption messages would be protected, however, it is not clear how this can be achieved since end-to-end encryption cannot be lifted on demand. The agreed text has not yet been published.

## 2.3. The Online Safety Act in the UK

### 2.3.1. Introduction

This subsection will analyse the key provisions in the United Kingdom (UK) Online Safety Act (OSA), focusing primarily on how this statute seeks to regulate online content relating to the trafficking of human beings (THB) and child sexual abuse and exploitation (CSA/E). The OSA was first introduced by government as a bill before the Houses of Parliament on 17th March 2022,[8] and has since undergone First, Second and Third Reading in both the House of Commons and the House of Lords. Following various debates and consideration of amendments to the text,[9] it was announced on 19th September 2023 that an agreement between the two Houses had been reached on the final drafting,[10] following which on 26th October 2023, the Bill received Royal Assent and was enacted as the OSA. Initially introduced as a Government Bill, the principal legislative intention of the OSA is to improve the safety of internet services in the UK, in particular for children.[11] The origins of this central aim can be traced to the Government's Internet Safety Strategy (2017-18), which ambitiously set out to make Britain "the safest place to be online".[12] To this end, the OSA imposes duties on regulated providers "to identify, mitigate and manage the risks of harm" arising from illegal content and activity, and content and activity that is harmful to children.[13] The specified aim of imposing such duties is primarily to ensure that regulated services are "safe by design" and operated in such a way that a higher standard of protection is provided for children compared with adults.[14] In addition, these duties aim to guarantee users' rights to privacy and freedom of expression, and to promote transparency and accountability

[6] EURACTIV October 23, EU Parliament nails down agreement on child sexual abuse regulation: https://www.euractiv.com/section/law-enforcement/news/eu-parliament-nails-down-agreement-on-child-sexual-abuse-regulation/
[7] MEPs reach political agreement to protect children and privacy: https://iptegrity.com/index.php/european-union/privacy/1160-european-parliament-tables-pragmatic-proposal-to-protect-children-on-line
[8] Online Safety Bill HC Bill (2021-22) 285.
[9] Online Safety Bill HL Bill (2022-23) 170.
[10] Department for Science, Innovation and Technology and The Rt Hon Michelle Donelan MP, 'Britain makes internet safer, as Online Safety Bill finished and ready to become law', *GOV.UK*, (2023). https://www.gov.uk/government/news/britain-makes-internet-safer-as-online-safety-bill-finished-and-ready-to-become-law.
[11] Online Safety Act 2023, s 1(1).
[12] HM Government, 'Government response to the Internet Safety Strategy Green Paper', *GOV.UK*, (2018), https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper#full-publication-update-history
[13] Online Safety Act 2023, s 1(2)(a)(i)-(ii).
[14] Online Safety Act 2023, s 1(3)(a)-(b)(i).

 

in relation to the provision of services.[15] Yet, as discussed further below, these various aims may be brought into conflict as a result of a potentially far-reaching clause within the statute that some prominent critics have argued could lead to mandated mass surveillance of all digital communications by firms in the private sector.[16]

### 2.3.2. Regulated entities

There are three types of "regulated service"[17] within the scope of the OSA. The first are providers of "user-to-user services", defined as "an internet service by means of which content that is generated directly on the service by a user of the service, or uploaded to or shared on the service by a user of the service, may be encountered by another user, or other users, of the service."[18] Services with such 'functionality',[19] which, rather than actual sharing of particular content, represents the threshold for definition as such, includes social media platforms, instant messaging apps, and other online forums. The second are providers of "search services", which refers to "an internet service that is, or includes, a search engine".[20] By definition, this includes dedicated search engines such as Google and Bing, in addition to internet services not regulated as user-to-user services that provide a search function enabling a person to search across more than one website or database.[21] The third type of regulated entity are service providers of certain pornographic content,[22] as subject to the duties listed in Part 5, which include use of age verification and/or age estimation measures to ensure "that children are not normally able to encounter content that is regulated provider pornographic content in relation to the service."[23]

Focusing on the first two types of service providers, a necessary condition of being "regulated" and a "Part 3 service" within the meaning of the Act is that these user-to-user or search service providers have "links with the United Kingdom",[24] as evidenced, for example, by a significant number of UK users,[25] or the UK being one of or the only target market for the service.[26] In the alternative, such service providers will also fall within the scope of the Act if "the service is capable of being used in the United Kingdom" and "there are reasonable grounds to believe that there is a material risk of significant harm to individuals" in the UK from user-generated or search service content.[27] This has the effect of widening the purview of the OSA and enabling extra-territorial application.[28]

### 2.3.3. Duties of care

Part 3 of the OSA sets out the duties applicable to providers of regulated user-to-user services and regulated search services. In relation to the former, there are a core set of duties to which all service providers are

[15] Online Safety Act 2023, s 1(3)(b)(ii)-(ii).
[16] See, e.g., Amnesty International, 'UK: 'Spy clause' in Online Safety Bill must be addressed before it becomes law', (5th September 2023), https://www.amnesty.org.uk/press-releases/uk-spy-clause-online-safety-bill-could-lead-mass-surveillance
[17] Online Safety Act 2023, s 4(4)(a)-(c).
[18] Online Safety Act 2023, s 3(1).
[19] Online Safety Act 2023, s 3(2)(a).
[20] Online Safety Act 2023, s 3(4).
[21] Online Safety Act 2023, s 229.
[22] Online Safety Act 2023, s 79.
[23] Online Safety Act 2023, s 81.
[24] Online Safety Act 2023, s 4(2)(a).
[25] Online Safety Act 2023, s 4(5)(a).
[26] Online Safety Act 2023, s 4(5)(b).
[27] Online Safety Act 2023, s 4(6)(a)-(b).
[28] Online Safety Act 2023, s 204.

subject.[29] These include illegal content risk assessment duties,[30] safety duties to, amongst others, prevent individuals from encountering illegal content and establish systems and processes to remove such content,[31] and duties about freedom of expression and privacy.[32] Additional duties will apply to providers of particular kinds of regulated user-to-user services, according to whether they are likely to be accessed by children,[33] are classified as Category 1 services[34] (as assessed by Ofcom, the UK media regulator, on the basis of regulations specifying threshold conditions introduced by the Secretary of State for Science, Innovation and Technology),[35] or are providers of combined services.[36] The duties with which regulated providers of search services must comply are similarly structured, with all providers subject to a range of duties mirroring those of user-to-user service providers,[37] including those relating to illegal content,[38] content reporting,[39] and complaints procedures,[40] and further obligations imposed on the providers of services "that are likely to be accessed by children",[41] in accordance with the underlying policy objective of greater protection for children. In general, providers of Part 3 services are "to be treated as complying with a relevant duty if the provider takes or uses the measures described in a code of practice which are recommended for the purpose of compliance with the duty in question."[42] These codes of practice relating to particular duties are to be prepared and published by the empowered regulator, namely the UK's communications regulator, Ofcom, and will include, for example, guidance on specific measures to be taken for the purposes of compliance with duties relating to illegal CSA/E content or offences.[43]

### 2.3.4. Illegal content

As noted above, a primary duty to which all regulated user-to-user and search service providers are subject relates to the design or operation of a service to "prevent individuals encountering priority illegal content by means of the service" and to "effectively mitigate and manage" both the risk of the service being used for the purposes of commissioning or facilitating a priority offence and the risk of harm to individuals, as identified in an illegal content risk assessment.[44] "Illegal content", as defined in the Act, refers to "content consisting of certain words, images, speech or sounds", the use, possession, viewing, accessing, publication or dissemination of which amounts to a "relevant offence".[45] Relevant offences are listed as either "a priority offence" or an offence under subsection (5),[46] with the former category comprising three main typologies, namely terrorism offences,[47] offences related to CSA/E,[48] and "other priority offences",[49] including THB.[50] Duties of care resulting from this classification include that regulated user-to-user providers, for instance, are required to

[29] Online Safety Act 2023, s 7(2)(a)-(f).
[30] Online Safety Act 2023, s 9.
[31] Online Safety Act 2023, s 10(2)-(3).
[32] Online Safety Act 2023, s 22.
[33] Online Safety Act 2023, s 7(4); s 37.
[34] Online Safety Act 2023, s 7(5).
[35] Online Safety Act 2023, s 95.
[36] Online Safety Act 2023, s 7(6).
[37] Online Safety Act 2023, s 24(2).
[38] Online Safety Act 2023, s 24(2)(b); s 27(2)-(8).
[39] Online Safety Act 2023, s 24(2)(c); s 31.
[40] Online Safety Act 2023, s 24(2)(d); s 32.
[41] Online Safety Act 2023, s 24(4).
[42] Online Safety Act 2023, s 49(1).
[43] Online Safety Act 2023, s 41(2).
[44] Online Safety Act 2023, s 10(2)(a)-(c).
[45] Online Safety Act 2023, s 59(3)(a)-(c).
[46] Online Safety Act 2023, s 59(4)(a)-(b).
[47] Online Safety Act 2023, s 59(7)(a); sch 5.
[48] Online Safety Act 2023, s 59(7)(b); sch 6.
[49] Online Safety Act 2023, s 59(7)(c); sch 7.
[50] Online Safety Act 2023, sch 7(24)-(26).

 

specify in their terms of service agreements how users will be protected from illegal content including both CSA/E and THB,[51] while regulated providers of search services will need to operate their services "using proportionate systems and processes designed to minimise the risk of users encountering search content" pertaining to priority illegal content, such as CSA/E content, or any other illegal content it "knows about".[52]

### 2.3.5. E-Evidence Investigations: Child sexual exploitation and abuse offences

A key provision in the OSA relating to the criminal investigation of online CSA/E is the introduction of a statutory duty for providers of regulated user-to-user and search services to report "all detected and unreported CSA/E content present on the service" to the National Crime Agency (NCA).[53] This mandatory reporting requirement builds on the existing voluntary regime under the auspices of the Interim Code of Practice on Online Child Sexual Exploitation and Abuse,[54] which was published by the Government as part of its response to the initial 'Online Harms' White Paper consultation.[55] Both UK and non-UK-based providers are subject to compliance with this provision, the latter of which must only report "UK-linked CSA/E content",[56] namely that which is supported by evidence such as the place where the content was published or shared, or the nationality of a person suspected of committing the related offence.[57] The particular requirements regarding these reports, such as the information to be included, the timeframe, and records that providers must keep,[58] including the data associated with a report,[59] will be the subject of regulations created by the Secretary of State for Science, Innovation and Technology in consultation with the NCA and Ofcom, amongst other bodies.[60]

As a response to the "growing threat presented by online CSA/E",[61] the introduction of a compulsory reporting system has been welcomed by civil society organisations, including children's charities such as National Society for the Prevention of Cruelty to Children (NSPCC), as well as law enforcement agencies (LEAs), such as the NCA. While the latter has supported the overall reporting regime as a mechanism to "ensure law enforcement receives the high quality information it needs to safeguard children and pursue offenders,"[62] the former has gone further by advocating in favour of a proposed amendment to the Bill during drafting which would see individuals held criminally liable for failure to comply with the requirement to report CSA/E content, alongside all other enforceable requirements.[63] However, as a result of the Government's desire to strike more of a balance between "holding people accountable for their actions in a way which is effective and targeted towards child safety, whilst ensuring the UK remains an attractive place to invest and grow",[64] the OSA eschews introducing comprehensive criminal liability for individuals. Instead, the Act provides that individuals may be held criminally liable only in specified instances. These include certain so-called

[51] Online Safety Act 2023, s 10(5).
[52] Online Safety Act 2023, s 27(3)(a)-(b).
[53] Online Safety Act 2023, s 66(1).
[54] Department for Culture, Media & Sport, Home Office, and Department for Digital, Culture, Media & Sport, 'Interim code of practice on online child sexual exploitation and abuse', *GOV.UK*, (2020), https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice
[55] John Woodhouse, Sally Lipscombe and Lorraine Conway, 'Analysis of the Online Safety Bill', *House of Commons Library*, (2022) https://commonslibrary.parliament.uk/research-briefings/cbp-9506/
[56] Online Safety Act 2023, s 66(2).
[57] Online Safety Act 2023, s 70(6)(a)-(d).
[58] Online Safety Act 2023, s 67(2)(a)-(f).
[59] Online Safety Act 2023, s 67(4)(a)-(b).
[60] Online Safety Act 2023, s 67(5)(a)-(c).
[61] Department for Digital, Culture, Media & Sport and Home Office, 'Online Harms White Paper', *GOV.UK*, (8th April 2019), https://www.gov.uk/government/consultations/online-harms-white-paper
[62] National Crime Agency, 'New reporting regime for online child sexual abuse content announced', (17th March 2022), https://www.nationalcrimeagency.gov.uk/news/new-reporting-regime-for-online-child-sexual-abuse-content-announced
[63] See, e.g., NSPCC, 'Parliamentary Briefing: Report Stage of the Online Safety Bill', (July 2022), https://www.nspcc.org.uk/globalassets/documents/policy/online-safety-bill-report-stage-parliamentary-briefing.pdf
[64] Michelle Donelan, 'Online Safety Update', 17 January 2023, HCWS500, https://questions-statements.parliament.uk/written-statements/detail/2023-01-17/hcws500.

"information offences",[65] certain offences committed by "a body corporate" with the consent, connivance or neglect of a corporate officer,[66] and the offence of failure to comply with a requirement imposed in a "confirmation decision" issued by Ofcom.[67]

The first is most relevant for present purposes and arises in relation to Ofcom's power to issue an "information notice" requiring information for the purposes of assessing, inter alia, the requirement to report CSA/E content,[68] for which there may be an additional requirement imposed for the provider to name in their response to a notice a senior manager "who may reasonably be expected to ensure compliance with the requirements of the notice."[69] Named senior managers will then be held criminally liable where, without a relevant defence,[70] they have "failed to take all reasonable steps" to prevent the entity from committing an information offence, such as failing to comply with an information notice or providing false or encrypted information.[71] In addition, a person will be found to have committed an offence if, in purported compliance with the requirement to report CSA/E content, information is provided that "the person knows is or is reckless as to whether it is false in a material respect."[72] Hence, the basis for individual criminal liability in relation to this provision is for failings around the procedural aspect of compliance, rather than the more substantive failure to discharge the requirement to report, which is enforceable against the *providers* of regulated services.[73] Still, a person may be found to have committed an offence for a failure to discharge a more substantive safety duty about illegal content, such as to prevent individuals from encountering CSA/E content by means of the service, but this is subject to Ofcom issuing a "confirmation decision" specifying the so-called CSA/E requirement with which the individual then fails to comply.[74] The next subsection will build on this by further assessing the scope and potential effects of Ofcom's suite of enforcement powers, focusing in particular on the potential ethical trade-offs associated with its power to issue notices requiring regulated service providers to deal with CSA/E content.

### 2.3.6. Enforcement

The OSA grants various new functions and powers to the regulator Ofcom to enforce the regulatory framework,[75] one of the most contentious of which relates to the communications regulators' ability to issue notices to regulated providers of user-to-user or search services requiring that they deal with CSA/E content.[76] Under the terms of the Act, "if Ofcom consider that it is necessary and proportionate to do so",[77] they may issue a notice requiring that regulated user-to-user service providers "use accredited technology" to identify, remove and/or prevent individuals from encountering CSA/E.[78] Significantly, the remit of this requirement to scan for CSA/E content using "accredited technology", defined as "meeting minimum standards of accuracy"[79] in the detection of prohibited content, applies whether "communicated publicly or privately by means of the service".[80] The far-reaching scope of this provision has sparked a debate around the balance struck between two overarching and potentially competing aims of the Act, namely to safeguard and protect children from

[65] Online Safety Act 2023, s 110.
[66] Online Safety Act 2023, s 186.
[67] Online Safety Act 2023, s 138.
[68] Online Safety Act 2023, s 100(6)(a)(iii).
[69] Online Safety Act 2023, s 103(2).
[70] Online Safety Act 2023, s 110(3); s 110(7)-(9).
[71] Online Safety Act 2023, s 110(2)-(6).
[72] Online Safety Act 2023, s 69(1)(a)-(b).
[73] Online Safety Act 2023, s 131(2).
[74] Online Safety Act 2023, s 138(3).
[75] Online Safety Act 2023, s 1(2)(b).
[76] Online Safety Act 2023, s 121.
[77] Online Safety Act 2023, s 121(1).
[78] Online Safety Act 2023, s 121(2)(a)(iii)-(iv).
[79] Online Safety Act 2023, s 125(12)-(13).
[80] Online Safety Act 2023, s 121(2)(a)(iii)-(iv).

 

online harms including CSA/E, on the one hand, and to uphold all service users' privacy and security, on the other.[81]

In support of this provision, the NSPCC has argued that there is significant public support for safety measures to protect children from abuse online,[82] citing polling by YouGov finding that seven in ten UK adults agree with the requirement to use accredited technology to identify CSA/E in private messaging apps if a significant risk to children has been identified.[83] In comparison, the director of Amnesty Tech, an arm of one of the foremost global human rights organisations, Amnesty International, has dubbed this provision a "Spy Clause", suggesting it "could see the private sector being mandated to carry out mass surveillance of private digital communications."[84] A number of industry actors providing secure messaging services have also voiced concerns that compliance with such a notice could lead to enforced undercutting of end-to-end encryption.[85] In April 2023, for instance, a number of private messaging services, including WhatsApp and Element, signed an open letter in which they argued that the Bill could enable "Ofcom to try to force the proactive scanning of private messages", thereby "nullifying the purpose of end-to-end encryption as a result and compromising the privacy of all users."[86] Yet, whilst increasingly viewed as a key safeguard for the protection of human rights in digital and online environments, the use of end-to-end encryption by providers of secure messaging services has also been criticised for hindering LEAs' ability to identify, investigate, and prosecute CSA/E offenders.[87]

The Government's position, as outlined in its response to the Joint Committee report on the draft Online Safety Bill, is that "[e]nd-to-end encryption should not be rolled out without appropriate safety mitigations, for example, the ability to continue to detect known CSA/E imagery."[88] In similar vein, the NSPCC has previously called for Meta to put on hold plans to establish end-to-end encryption of Facebook and Instagram messenger services, advocating that "[t]he Online Safety Bill should be seen as an opportunity to encourage companies to invest in technological solutions to end-to-end encryption that protect adult privacy and keep children safe."[89] Nonetheless, the possibility of developing technology that simultaneously enables scanning for prohibited content while also maintaining end-to-end encryption has been rejected by a group of security and privacy experts in an open letter published in July 2023. Here, they argue that "[t]here is no technological solution to the contradiction inherent in both keeping information confidential from third parties and sharing

[81] Ian Levy and Crispin Robinson, 'Thoughts on child safety on commodity platforms', *arXiv*, (2022), https://doi.org/10.48550/arXiv.2207.09506.
[82] NSPCC, 'Online Safety Bill Briefing: Consideration of Lords Amendments – House of Commons', (September 2023), https://www.nspcc.org.uk/globalassets/documents/online-safety/nspcc-online-safety-bill-brief---sept-23.pdf
[83] NSPCC, 'Public backs action to prevent child abuse in private messaging', (5th July 2023), https://www.nspcc.org.uk/about-us/news-opinion/2023/Public-backs-action-to-prevent-child-abuse-in-private-messaging/
[84] Amnesty International, 'UK: 'Spy clause' in Online Safety Bill must be addressed before it becomes law', (5th September 2023), https://www.amnesty.org.uk/press-releases/uk-spy-clause-online-safety-bill-could-lead-mass-surveillance
[85] Benjamin Dowling, 'The UK just passed an online safety law that could make people less safe', *The Conversation*, (25th September 2023), https://theconversation.com/the-uk-just-passed-an-online-safety-law-that-could-make-people-less-safe-213595
[86] Matthew Hodgson et al., 'An open letter', *WhatsApp Blog*, (17th April 2023), https://blog.whatsapp.com/an-open-letter?lang=en
[87] See, e.g., National Crime Agency, 'Global law enforcement coalition urges tech companies to rethink encryption plan that put children in danger from online abusers', 19th April 2023, https://www.nationalcrimeagency.gov.uk/news/global-law-enforcement-coalition-urges-tech-companies-to-rethink-encryption-plans-that-put-children-in-danger-from-online-abusers
[88] Department for Digital, Culture, Media & Sport and Department for Science, Innovation & Technology, 'Government response to the Joint Committee report on the draft Online Safety Bill', *GOV.UK*, (17th March 2022), https://www.gov.uk/government/publications/joint-committee-report-on-the-draft-online-safety-bill-government-response/government-response-to-the-joint-committee-report-on-the-draft-online-safety-bill
[89] NSPCC, 'We're calling for effective action in the Online Safety Bill as child abuse image crimes reach record level', (22nd February 2023), https://www.nspcc.org.uk/about-us/news-opinion/2023/2023-02-22-were-calling-for-effective-action-in-the-online-safety-bill-as-child-abuse-image-crimes-reach-record-levels/

that same information with third parties."[90] In surveying the two main technological solutions proposed, namely cryptography and so-called "client-side scanning" (CSS), the signatories contend that these are either vulnerable to misuse by both State and non-State actors, or are otherwise lacking reliability to accurately and exclusively detect known prohibited content.[91] The British Computer Society has similarly argued that "any foreseeable technology would compromise privacy."[92] Amongst other things, this highlights that the relevant technology is as yet unproven; an indication of which is also present in the language of the statute, which requires providers to use their "best endeavours to develop or source technology" to help identify, remove and/or prevent CSA/E content.[93]

Following fierce debate around this provision, a late amendment to the Act, as introduced by the House of Lords and accepted by the House of Commons, stipulates that Ofcom are only able to issue a notice "after obtaining a report from a skilled person", which is to be used in deciding whether to issue a notice and in assessing the particular requirements attached to it.[94] Ofcom is also directed to consider a number of matters "in deciding whether it is necessary and proportionate to give a notice",[95] including potential for interference with rights to privacy and freedom of expression, and the possible chilling effect on journalism.[96] In addition to these textual mitigations against the concerns of overreach, there has also been a softening in the rhetoric used by government in relation to this provision. During a debate on Third Reading of the Bill in the House of Lords, for instance, the Parliamentary Under-Secretary of State of Department for Culture, Media and Sport, Stephen Parkinson, stated that "[a] notice can be issued only where technically feasible and where technology has been accredited as meeting minimum standards of accuracy in detecting only child sexual abuse and exploitation content."[97] He further explained that "if the appropriate technology does not exist that meets these requirements, then Ofcom will not be able to use [this Clause] to require its use."[98] Whilst intended to allay concerns that service providers could be forced under threat of sanction to deploy as yet unproven technology to scan users' messages, it was also pointed out by Lord Moylan that, whereas the use of only "accredited" technology is stipulated in the text of the Act,[99] the requirement of "technical feasibility is not built into the clause".[100] Indeed, while Ofcom is directed to consider "technically feasible measures" in developing codes of practice relating to the varies duties of care described above,[101] there is no such textual requirement relating to the issuing of notices to deal with CSA/E content. Thus, whilst it might be expected that Ofcom is likely to be guided by this principle, there is no explicit guarantee against a notice being issued irrespective of technical feasibility and potentially resulting in enforcement action being taken for failure to comply.[102] In consequence, much will depend on how Ofcom chooses to interpret and apply this provision in practice. Following the enactment of the Online Safety Act in October 2023, the regulator announced that as part of a three-phase approach to implementation it will firstly publish draft codes and guidance on compliance with so-called illegal harm duties in November 2023, which will be subject to consultation before finalisation by Autumn 2024.[103]

---

[90] Martin Albrecht and Hamed Haddadi et al., 'Open Letter from Security and Privacy Researchers in relation to the Online Safety Bill', https://haddadi.github.io/UKOSBOpenletter.pdf
[91] Ibid.
[92] The Chartered Institute for IT, 'The Online Safety Bill and the role of technology in child protection', (31st August 2023), https://www.bcs.org/media/10993/online-safety-bill-and-the-role-of-technology-in-child-protection.pdf.
[93] Online Safety Act 2023, s 121(2)(b)(i).
[94] Online Safety Act 2023, s 122.
[95] Online Safety Act 2023, s 124.
[96] Online Safety Act 2023, s 124(2)(a)-(j).
[97] HL Deb 6 September 2023, vol 832, col 458. Available at: https://hansard.parliament.uk/lords/2023-09-06/debates/4AC6A32E-0C53-46C7-A714-AD4165C484D7/OnlineSafetyBill
[98] HL Deb 6 September 2023, vol 832, col 458. Available at: https://hansard.parliament.uk/lords/2023-09-06/debates/4AC6A32E-0C53-46C7-A714-AD4165C484D7/OnlineSafetyBill
[99] Online Safety Act, s 125(12)-(13).
[100] HL Deb 6 September 2023, vol 832, col 458. Available at: https://hansard.parliament.uk/lords/2023-09-06/debates/4AC6A32E-0C53-46C7-A714-AD4165C484D7/OnlineSafetyBill
[101] Online Safety Act 2023, s 41.
[102] Ibid.
[103] Ofcom, 'Ofcom's approach to implementing the Online Safety Act', (26th October 2023), https://www.ofcom.org.uk/online-safety/information-for-industry/roadmap-to-regulation.

 

# 3. Legislative developments for LEAs

## 3.1. Transatlantic Agreements on cross-border access to e-evidence

### 3.1.1. The problem

Electronic evidence, or **'e-evidence'**, refers to **digital data** that is used to investigate and prosecute criminal offences. It may include e-mails, text messages, photographs and videos, traffic information, location data, information on user accounts etc. which is held by online service providers rendering services to end-users, such as Google, Instagram, or WhatsApp. Many of these service providers are located – along with the data they hold – in places where the LEAs investigating the case have no jurisdiction. It is estimated that "*e-evidence is needed in around 85% of criminal investigations, and in two-thirds of these investigations there is a need to request evidence from online service providers based in another jurisdiction."*[104]

Traditionally, LEAs have relied on mutual legal assistance routes signed in international treaties or even diplomacy channels (see HEROES D3.3), however, the process from when a request is made until it is fully processed, oftentimes takes too and LEAs have been facing great difficulties in obtaining e-evidence in a timely and efficient manner. Long waiting times to acquire e-evidence jeopardise the capacity of LEAs to investigate, detect and prosecute all sorts of crimes. On the other hand, e-evidence requests shall be processed with appropriate safeguards to pay utmost respect to the fundamental rights to privacy and data protection.

To solve this problem, LEAs have relied on bilateral cooperation agreements with service providers which are entirely voluntary and limited in scope, however the problem needed legislative action and the assurance of the rule of law. At EU level, the Commission proposed in 2018 the e-evidence package which after much debate has been approved last June 2023 by the European Parliament and published in the European Journal in July 2023 (see section 3.3 and D3.3 for further information). The novelty, after much doubt and criticism to effectively safeguard privacy and data protection while allowing LEAs to exercise their investigative duties efficiently, is that LEAs will be able to request e-evidence to service providers which are based abroad without directly involving, in most cases, the judicial authorities of the country where the service provider is located.

However, the initial problem will not be entirely addressed and solved by the e-evidence package. Major online service providers typically process and store end-users' data, including content data, in different jurisdictions outside the EU boundaries and more specifically content data is typically stored in the US. As part of the research conducted in this project, LEAs in the HEROES consortium have been interviewed to understand what their difficulties are. LEAs have expressed that acquiring content data from the US can take months if not years, unless there is an emergency, a threat to the life of individuals or national security. It is estimated that 'the number of requests to the main online service providers grew by 70% in the period between 2013 and 2016'[105].

This specific context has given rise to numerous international initiatives. The following sections explore the legal framework in the US and EU governing data sharing with foreign entities and the treaties signed and currently under negotiation with the US.

### 3.1.2. The CLOUD Act in the US

The Clarifying Lawful Overseas Use of Data Act (the "**CLOUD Act**") is a United States ("US") federal law enacted in 2018 which primarily amends the Stored Communications Act **("SCA")** of 1986 with the purpose to '*improve procedures for both foreign and US investigators in obtaining access to electronic information*

[104] European Commission, press release April 2018, FAQs: New rules to obtain electronic evidence: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
[105] Ibid

*held by service providers'*[106]. The government of the US acknowledges that the number of mutual assistance requests to service providers that hold the information in US soil, has increased 'dramatically'[107] in recent years and that there is a need to work more efficiently and faster.

The CLOUD Act allows the US to enter into bilateral and reciprocal agreements with other countries that have robust privacy laws for the mutual access to e-evidence directly from service providers.

### 3.1.3. The Umbrella Agreement in the EU

In October 2015, the Court of Justice of the EU ('**CJEU**') rendered invalid the EU-US Safe Harbor Framework in its ruling commonly known as '*Schrems I*'. The ruling marked a breaking point following the mistrust on personal data flows from the EU to the US officially sparked after Edward Snowden's surveillance revelations.

Nevertheless, political and legal actions to bring back trust in transatlantic data flows quickly followed. In July 2016, the EU-US Privacy Shield came into effect as a quick replacement of the Safe Harbor, which was rendered invalid after a year; and in December 2016, the US and the EU signed the 'Agreement on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences[108]' (the so-called '**Umbrella Agreement'**), establishing standards and safeguards in the protection of personal data when transferred amongst LEAs in the EU and the US. Furthermore, the Privacy Shield was rendered invalid by the CJEU in July 2020, but the Umbrella Agreement is still in force.

The Umbrella Agreement complements rules regarding personal data protection in the exchange of information in the investigation and prosecution of crimes. The Umbrella Agreement 'does not authorise any transfers of data but rather articulates safeguards in the event of a transfer between LEAs', therefore the Agreement does not establish any baseline for cooperation between judicial and police authorities from the EU and the US on the access and reciprocal exchange of e-evidence, its scope is limited to introducing safeguards in case that exchange occurs.[109] It should be noted that the Umbrella Agreement does not constitute a legal basis for personal data transfers to the US. However, the 'EU-US agreement on access to e-evidence' aims to provide said legal basis (see next subsection for further detail).

The Umbrella Agreement introduces a specific purpose limitation, insofar as the data shall only be used for the purpose of preventing, investigating, detecting and prosecuting criminal offences. It establishes restrictions on onward transfers, i.e., any further transfer to a third country may only be carried out if authorised by the initial issuing country. It also, includes judicial redress, the right to access and rectification of personal data (not present in US federal law), retention periods and notifications in case of data breaches.[110] The Umbrella Agreement does not replace but supplements other international agreements on the matter such as the EU-US Mutual Legal Assistance Agreement (2003) and the EU-US Agreement on airline passenger names record data.

[106] The Purpose and Impact of the CLOUD Act - FAQs: https://www.justice.gov/criminal-oia/page/file/1153466/download
[107] Ibid
[108] Council Decision (EU) 2016/920 of 20 May 2016 on the signing, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016D0920 and Umbrella Agreement: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A22016A1210%2801%29
[109] Jessica Shurson, Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law, International Journal of Law and Information Technology, 2020
[110] Eur lex summary of EU-US agreement on personal data protection: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8

 

### 3.1.4. EU-US agreement on access to e-evidence in criminal investigations

Negotiations between the US and the EU on an agreement to access e-evidence data started back in 2019, however, the negotiations were paused while the EU finalised the approval of the e-evidence package.

Now that the e-evidence package (see D3.3 for further information) has been adopted and published in the journal of the EU as Regulation on the 28th of July 2023 as "*Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings*" (also called '**E-evidence Regulation')**[111] and **"***Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings*" (also called '**E-evidence Directive'),** the negotiations between the EU and the US have been resumed.[112]

Turning back to 2019, the Council issued a recommendation authorising the EC to negotiate on behalf of the EU regarding the agreements with the US on cross-border access by judicial authorities in criminal proceedings to e-evidence held by a service provider[113] (the '**Recommendation'**). The Annex to the Recommendation lays down the objectives that the EC should seek in such negotiations and defines the nature, scope, safeguards and governance of the agreement, this way, Section 2 of the Annex provides:

1. *The agreement should apply to criminal proceedings which include both pre-trial and trial phases.*
2. *The agreement should create reciprocal rights and obligations of the parties.*
3. *The agreement should set out the definitions and types of data that are to be covered, including both content and non-content data.*
4. *The agreement should define its exact scope of application in terms of the criminal offences covered and the thresholds.*
5. *The agreement should set out what the conditions are to be met before a judicial authority can issue an order and the ways in which an order can be served.*
6. *The agreement should include a clause enabling effective judicial remedies for data subjects during criminal proceedings. The agreement should also define in which circumstances a service provider has the right to object to an order.*
7. *The agreement should define the time period for supplying the data covered by the order.*
8. *It should be without prejudice to other existing international agreements on judicial cooperation in criminal matters between authorities, such as the EU-U.S. Mutual Legal Assistance Agreement.*
9. *The agreement should, in the bilateral relations between the Union and the United States of America,* ***take precedence over the Council of Europe Convention on Cybercrime*** *and any agreement or arrangement reached in the negotiations of the* ***Second Additional Protocol*** *to the Council of Europe*

[111] E-evidence Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543
[112] EC, March 23, EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations: https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en
[113] Council of the EU, Feb 2019, Recommendation for a COUNCIL DECISION authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019PC0070

*Convention on Cybercrime, in so far as the provisions of the latter agreement or arrangement cover issues dealt with by the agreement.*

As far as safeguards to the fundamental rights and freedoms of individuals are concerned, the agreement shall include the application of the safeguards enshrined in the Umbrella Agreement and it shall include further safeguards, such us the specification of purposes and proportionality test. There are several points that are sparking dissent during the negotiations, which most likely include but are not limited to (1) the introduction of prior authorisation by the judicial competent authority in the EU of any data use and disclosure to other US authorities bound by the Umbrella Agreement; (2) prior authorisation by the EU judicial authorisation for onwards transfers to third-countries, except in cases of imminent threat to public security, (3) the exclusion of data requested for the use in criminal proceedings which might lead to the death penalty.

After both parties have agreed on a draft agreement, the European Parliament will have to give its consent to the text, after which the Council will have to adopt a final decision. The European Data Protection Supervisor ('**EDPS**') was already consulted in 2019 and will have to be consulted again on the text of the draft agreement.

As seen in point 3 listed above, the Agreement should apply to content and non-content data. Access to content data interferes with the fundamental right of secrecy of communications enshrined in Article 7 of the Charter of Fundamental rights of the EU and protected at constitutional level in most EU Member States. Any interference with the right to secrecy of communications is considered an interception of private communications and can only be carried out by police forces upon prior judicial authorisation, for instance wiretapping or access to the content of letters or emails.

In practice and to a certain extent, direct cooperation from EU LEAs with service providers located in the US already exists, but this cooperation only pertains to non-content data and is voluntary carried out by service providers. Same voluntary cooperation applies to the access to cross-border e-evidence within EU Member States and will be mandatory with the approval of the E-evidence Directive and Regulation (see HEROES D3.3) which were only published in the journal of the EU on 28th July 2023, and which shall be applicable in the upcoming years.

The negotiation agreement seeks to implement direct cooperation with US service providers whereby EU LEAs could obtain content and non-content data directly from them without the need to seek US prior judicial authorisation and vice versa, LEAs in the US could obtain data directly from EU service providers. In addition, and according to EU data protection law international data transfers from EU service providers or LEAs always need a legal basis and the EU-US agreement aims at providing such legal basis.

The EDPS issued its Opinion on the negotiating mandate of an EU-US agreement on cross border access to electronic evidence (Opinion 2/2019) whereby, amongst others, recommended clarification in the text of the Recommendation regarding whether the prior authorisation needed to use and disclose data relates solely to US authorities not bound by the Umbrella Agreement, or it also applies to the communication of the data from US authorities bound by the Umbrella Agreement to others which are not so bound. Notably, for the sake of effective protection of fundamental rights, the EDPS recommends inclusion of a '*degree of involvement of public authorities' of the country which receives the request for access data, more concretely, the systematic involvement of judicial authorities as early as possible 'in order to give these authorities the possibility to effectively review compliance of the orders with fundamental rights and possibly to raise grounds for refusal, on the basis of sufficient information and within realistic deadlines'*. This is the same approach taken by the E-Evidence Regulation whereby for traffic data and content data the issuing authority (requesting access to the e-evidence in another Member State) shall notify the enforcing authority of the State where the service provider is located, unless the offence is being committed or is likely to be committed in the issuing State and the person whose data is requested resided in the issuing State.[114] However, when this notification is pertinent, it will have

[114] Article 8 of the E-evidence Regulation

 

suspensive effects on the obligations of the service provider receiving the order to disclose the data except in emergency cases.

### 3.1.5. UK-US Agreement on access to e-evidence

The UK-US Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime [CS USA No.6/2019] – the '**UK-US Agreement'**[115] (or the 'Agreement' in this section) is the first agreement signed by the US authorised under the CLOUD Act. It was signed in October 2019 and the UK parliamentary scrutiny concluded it could be ratified in January 2020[116]. The Agreement entered into force in October 2022.[117]

The Agreement covers the exchange of content data, traffic data, subscriber data and account data and also investigative measures such as the interception of wire or electronic communications. The title of the Agreement refers to 'serious crimes' which might lead one to think that only crimes punished with long imprisonment sentences of several years are under its scope (for instance in Spain, manslaughter might be punished with 10 – 15 years). However, Article 1.14 defines '*serious crime'* as an '*offence that is punishable by a maximum term of imprisonment of at least 3 years'*, mirroring this way the E-evidence Regulation in the EU and which in practice will cover most of crimes.

Any order issued under the Agreement shall be subject to judicial review or oversight and might be issued directly to service providers in the jurisdiction of the other party, including a written certification that the order is lawful and complies with the Agreement. Service providers may rise objections which shall be responded by the issuing party's authorities. In case that the objections are not resolved, the service provider may rise this with the authority designated in its country (Article 5.11).

The Agreement confers special protection to 'US persons' which is a term defined in Article 1.16 as US nationals, residents and US corporations, which by the wording of the definition can be interpreted as being located in the US, the UK or anywhere in the world. The UK cannot access data of US persons, or a person located in the US, this is a condition sine qua non subsumed in the CLOUD Act[118]. However, the US can access data of UK persons not located in the UK, UK persons could be targeted as long as they are not in the UK. This imbalance and lack of reciprocity is justified in the Explanatory Memorandum to the Agreement published from the UK Foreign & Commonwealth Office stating that '*this differentiation results from EU law which prohibits discrimination in treatment between citizens of different member states'*. This Agreement was signed in October 2019 and the UK left the EU shortly after.

Further limitations are included in Article 8 of the Agreement whereby the UK might refuse to provide evidence when it can form part of criminal proceedings where the death penalty is sought; in such cases the issuing authority needs to obtain permission from the receiving authority in the UK. Similarly, US authorities shall be involved when data may be used during a case which may raise freedom of speech concerns. In terms of privacy safeguards, the Agreement specifically incorporates the application of the Umbrella Agreement.

[115] UK – US Agreement, Gov UK: https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019
[116] UK Parliament, Roadmap UK-US Agreement: https://api.parliament.uk/view/treaty/bjKV1oDq
[117] Office of public affairs U.S Department of Justice, Landmark US-UK Data Access Agreement Enters into Force: https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force
[118] Section 2523 (b). (2) and (3) of the CLOUD Act: https://www.congress.gov/bill/115th-congress/senate-bill/2383/text#:~:text=3)%20the%20agreement,the%20United%20States%3B

In practice, the Agreement still needs to prove its efficacy. Also in practice, the Agreement seems to facilitate the exchange of data in a one-way manner from the US to the UK, given the large proportion of service providers located in the US rendering services in the UK and the EU as a whole.[119]

### 3.1.6. Australia – US CLOUD Act Agreement

On 15 December 2021, the Australian Minister for Home Affairs and the US Attorney General signed the 'Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime', referred to as the '**Australia-US CLOUD Act Agreement**' or 'Agreement' in this section.[120] The Agreement is not yet in force. In June 2021, the Australian Parliament passed the Telecommunication Legislation Amendment (International Production Orders) Bill which enables Australia to comply with access request orders from foreign authorities. [121]

The Agreement with Australia is highly similar to the Agreement signed with the UK. Interestingly, it contains a definition of 'Australian person' whereas in the UK Agreement the definition of a UK person is missing which leads to the reciprocity that the UK Agreement lacks: neither the US nor Australia can request access to data about US persons and Australian persons respectively regardless of their place of location, whereas the UK- US Agreement provides for US authorities to target UK persons as long as they are not located in the UK.

As in the UK Agreement, limitations apply to the access of the US to data in proceedings for which the death penalty is sought and access to data by Australia where freedom of speech concerns may arise.

### 3.1.7. Conclusion

The chosen nomenclature of these international instruments to facilitate the exchange of data for law enforcement purposes is remarkable. They are formally called 'agreements' when the common practice is to name them international treaties. The reference to an agreement evokes an arrangement between private parties, however, this is far from reality; these instruments need to be signed and ratified by the States which participate as parties just like any other international treaty. However, it is also curious that in practice, it seems they are negotiated in the same way as agreements are negotiated amongst private parties. When private parties negotiate, usually the party offering to render its services to the other and the party with the strongest negotiation power issues its 'template'. In this context, the agreements signed with the UK and Australia have the same structure, with tailored clauses and changes made out of the negotiation process.

This fact has not gone unnoticed by the European Parliament, which submitted a set of questions to the EC after the signature of the UK – US Agreement, including the following: *Does the Commission consider that this agreement sets a precedent, or that it restricts the room for manoeuvre for EU negotiators?*[122] It is also open to question whether the UK-US Agreement is in line with the GDPR, the LED and the case law of the

[119] The globalisation of criminal evidence and the UK-US Data Sharing Agreement, BLC partners Michael Drury and Julian Hayes, M arch 2022: https://www.bcl.com/the-globalisation-of-criminal-evidence-and-the-uk-us-data-sharing-agreement/

[120] Australia-US CLOUD Act Agreement: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/australia-united-states-cloud-act-agreement#:~:text=The%20Australia%2DUS%20CLOUD%20Act%20Agreement%20is%20focussed%20on%20allowing,located%20in%20their%20own%20jurisdiction. Link to the Agreement: https://www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf

[121] Telecommunication Legislation Amendment (International Production Orders) Bill: https://parlwork.aph.gov.au/Bills/r6511

[122] Parliamentary Question: UK-US agreement under the US CLOUD Act, Oct 2019: https://www.europarl.europa.eu/doceo/document/E-9-2019-003136_EN.html

 

European Court of Human Rights. This question is pertinent in the context of the EU-US negotiations. Whether the EU-US agreement will be the same as the UK and Australia following the CLOUD Act framework is yet to be seen,[123] as is whether the US would conclude an EU agreement covering 27 States rather than bilateral agreements with Member States.

## 3.2.Directive 2023/977 for the exchange of information amongst LEAs

### 3.2.1. Introduction

Directive 2023/977 has been recently approved. It has been published in the Official Journal of the EU in May 23 and shall be transposed into national law by December 2024. It has repealed Framework Council Decision 2006/960/JHA on simplifying the exchange of information and intelligence among LEAs of the Member States of the European Union – the so-called '**Swedish Framework Decision'**- and establishes new rules for the adequate and rapid exchange of information for the prevention, detection, and investigation of criminal offences.

### 3.2.2. Scope and procedure for the exchange of information

The Directive introduces the obligation for Member States to designate '**Single Points of Contact**' which shall be the entities responsible for the coordination and facilitation of the exchange of information.

LEAs willing to obtain information from other LEA in another Member State shall submit a request to the Single Point of Contact of that Member State and send a copy to the designated Single Point of Contact in their country.

Single Points of Contact shall use Europol's Secure Information Exchange Network Application ('**SIENA**') to send requests for information, to provide information pursuant to such requests and to provide information on its or their own initiative. However, there are some exceptions to the use of SIENA:

- When the exchange of information requires the involvement of third countries or international organisations;
- When the urgency of the request for information requires to use an alternative system; and
- When there is a technical or operational incidence in the Single Point of Contact of the relevant country.

Member States shall establish a list of one or more languages in which their Single Point of Contact will operate and can be addressed, the only requirement is that English shall be included on the list, once the languages have been designated, the Commission will publish a compilation of the lists gathered within the Member States.

Pursuant to Article 3 all the exchanges of information shall be done in accordance with the following principles:

- **Principle of availability**: Single Points of Contact shall be established and operational as well as the LEAs which receive the requests.

- **Principle of equivalent access**: the conditions for requesting and providing information shall be equivalent to those applicable to LEAs within that Member State.

[123] Jessica Shurson, Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law, International Journal of Law and Information Technology, 2020

- **Principle of confidentiality**: information provided or requested that is marked as confidential shall be treated with the same level of confidentiality in that Member State.

- **Principle of data ownership:** where the requested information has been obtained initially from another Member Sate or a third country, the State replying to such information request shall only provide the information with the consent, or the conditions imposed by the country where the information came from.

- **Principle of data reliability**: personal data exchanged shall comply with Directive 2016/680, and data which is not accurate, incomplete, or updated shall be erased or rectified and the recipient shall be notified with undue delay.

The exchange of certain information might be subject to the judicial authorisation of the Member State receiving such request. In such cases, the requesting State shall be informed, and judicial authorisation sought.

### 3.2.3. Grounds for refusal

Requests for information can be refused under certain circumstances set out in Article 6, i.e., when:

- The procedural requirements are not met;
- The judicial authorisation has been refused;
- The information is not available;
- The information concerns categories of personal data not listed in Annex II, Section B of Directive 2016/794;
- There are reasons to believe that delivering such information could jeopardise national security, a criminal investigation or unduly harm the interests of a legal person;
- The request pertains to a criminal offence punishable by a maximum term of imprisonment of one year or less under the law of the requested Member State;
- A matter that does not constitute a criminal offence under the laws of the State receiving the request;
- The information in scope was initially obtained from another Member State or third country which has not consented to disclose such information.

## 3.3. The EU e-evidence package developments

The e-evidence package was analysed in detail as part of the HEROES project in D3.3. By way of update as referred above, the e-evidence packaged has been adopted and published in the journal of the EU in the form of a regulation and a directive. The regulation shall be fully applicable from August 2026 and the Directive on the designation of establishments and the appointment of legal representatives shall be transposed by Member States into national law by February 2026.

 

# 4. Legislative developments for technical partners

## 4.1. The AI Act

### 4.1.1. Progress and status

Efforts to regulate Artificial Intelligence ('**AI**') are being made all over the world in various forms, including identifying ethical principles that AI systems should follow, regulations and proposals for regulations.

Most of the tools developed by technical partners in HEROES rely to some extent or entirely on AI components. As such, we (TRI) have assessed the HEROES tools from the lens of the 7 principles for an ethical and trustworthy AI identified by the High-Level Expert Group on AI and published by the EC in 2019[124] in section 15 of deliverable D3.11.

The EC released its proposal to regulate AI in the EU in April 2021[125]. Since then, the text for the proposal have been revised by the European Council which released its version with amendments in December 2022[126]. Taking the Council's version as a basis, in section 4 of D3.2, we assessed whether the tools developed in HEROES would fall under the category of high-risk AI systems and identified in D3.5 what the obligations are for providers and end-users of high-risk AI systems, which in practice HEROES technical partners and the LEAs interested in acquiring such tools as end-users will need to comply with as part of the HEROES exploitation plan.

D3.2 was submitted in M18 of the project (May 2023) and soon after the submission date, the European Parliament ('**EP**') published its revised and amended version of the AI Act on the 23rd of May 2023). The EP's version is the version which is being discussed during the so-called trilogue negotiations between the Parliament, the Council and the Commission. Some of the amendments introduced by the EP are far-reaching and will have a direct impact on the AI governance of the HEROES tools. The sections below provide HEROES partners an update on the most substantial amendments that shall be monitored for future compliance and also further elaborate on some of the obligations.

### 4.1.2. General principles applicable to all AI systems

The compromise amendments by the EP included a new Article 4 (a) of the AI text proposal which establishes that all operators of the AI systems 'shall make their best efforts to develop and use the AI systems in accordance with the following general principles based on the principles for ethical and trustworthy AI identified by the High-Level Expert Group on AI':

a) **'human agency and oversight'** means that AI systems shall be developed and used as a tool that serves people, respects human dignity and personal autonomy, and that is functioning in a way that can be appropriately controlled and overseen by humans.
b) **'technical robustness and safety'** means that AI systems shall be developed and used in a way to minimize unintended and unexpected harm as well as being robust in case of unintended problems and being resilient against attempts to alter the use or performance of the AI system so as to allow unlawful use by malicious third parties.

[124] Ethics guidelines for trustworthy AI, EC 2029: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
[125] EC proposal for an AI Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206
[126] AI Act Proposal, version of the EU Council, December 2021: https://data.consilium.europa.eu/doc/document/ST-15698-2022-INIT/EN/pdf

c) **'privacy and data governance'** means that AI systems shall be developed and used in compliance with existing privacy and data protection rules, while processing data that meets high standards in terms of quality and integrity.
d) **'transparency'** means that AI systems shall be developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system as well as duly informing users of the capabilities and limitations of that AI system and affected persons about their rights.
e) **'diversity, non-discrimination and fairness'** means that AI systems shall be developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law.
f) **'social and environmental well-being'** means that AI systems shall be developed and used in a sustainable and environmentally friendly manner as well as in a way to benefit all human beings, while monitoring and assessing the long-term impacts on the individual, society and democracy

This way the EP's text seeks to make legally binding the principles of the High-Level Expert Group published in 2019. However, the wording is somehow unclear 'operators shall make best efforts', the provision, if approved as is, would make binding those principles to all AI systems, but a commitment to pursue best efforts seems to be the only requirement, leaving to the judgment of the operators whether the efforts shall shape the nature and core operations of the AI system or it will be a provision that can just not be fully complied with in case that there is a disproportionate effort involved for instance when the AI systems has already been designed and it is operating in the real world. Further guidance on how to interpret this provision will certainly be needed in the future, if not, it the extent and scope of the obligation contained will sooner or later be interpreted by the judiciary.

### 4.1.3. Falling under the high-risk category

The Commission and the Council's version of the AI Act provided a list of high-risk AI systems uses and categories in Annex III. Therefore, if the AI system would fall under one of those categories (law enforcement, border control, employment, etc.) - unless the output of the system is purely accessory[127]- the AI system would be automatically considered a high-risk AI system and therefore would need to comply with stricter rules.

Nonetheless, the EP's version introduced a new provision under Article 6.2:

*In addition to the high-risk AI systems referred to in paragraph 1, AI systems* ***falling under one or more*** *of* ***the critical areas and use cases*** *referred to in Annex III shall be considered high-risk* ***if they pose a significant risk of harm to the health, safety or fundamental rights of natural persons. Where an AI system falls under Annex III point 2, it shall be considered high-risk if it poses a significant risk of harm to the environment.***

***The Commission shall, 6 months prior to the entry into force of this Regulation, following consultation with the AI Office and relevant stakeholders, provide guidelines clearly specifying***

[127] Article 6.3 of the Council's version. The text did not specify when to consider the output purely accessory only recital 32 states: "*However, if the output of the AI system has only negligible or minor relevance for human action or decision, it may be considered purely accessory, including for example, AI systems used for translation for informative purposes or for the management of documents.*"

 

> ***the circumstances where the output of AI systems referred to in Annex III would pose a significant risk of harm to the health, safety or fundamental rights of natural persons or cases in which it would not.***

As a consequence of the wording of new Article 6.2, AI systems falling under one of the categories listed in Annex III will not be automatically categorised as a high-risk AI system in the way that the Commission's and the Council's versions provided, but only if those systems '***pose a significant risk of harm to the health, safety or fundamental rights of natural persons'***. In practice, this means, that AI providers and users will need to assess whether their AI systems pose a significant risk in the terms described, however, the text does not indicate how to conduct this assessment, although it is established that the EC will publish guidelines to indicating the circumstances where outputs can pose a high-risk only 6 months prior to the AI Act's date for entry into force. Without knowing the exact scope that these guidelines would cover, it is worth noting that it is not specified that the guidelines would cover how to perform this assessment, in practice, one might thing about ethical impact assessment or fundamental rights impact assessments, but the EC should be proactive in instructing the industry how this assessment might be carried out in accordance with the regulation for the sake of legal certainty.

### 4.1.4. Fundamental Rights Impact Assessment

The EP's version has also introduced under the new Article 29(a) an obligation for end-users of high-risk AI systems (in the case of HEROES, LEAs) to conduct a fundamental rights impact assessment prior to implementing and operationalising the AI system with the exception of those used for the management and operation of critical infrastructure (section 2 of Annex III). The aim is to establish the specific impact of the AI system in its context of use.

The fundamental rights impact assessment, shall include the following elements:

> a) a clear outline of the intended purpose for which the system will be used;
> b) a clear outline of the intended geographic and temporal scope of the system's use;
> c) categories of natural persons and groups likely to be affected by the use of the system;
> d) verification that the use of the system is compliant with relevant Union and national law on fundamental rights;
> e) the reasonably foreseeable impact on fundamental rights of putting the high-risk AI system into use;
> f) specific risks of harm likely to impact marginalised persons or vulnerable groups;
> g) the reasonably foreseeable adverse impact of the use of the system on the environment;
> h) a detailed plan as to how the harms and the negative impact on fundamental rights identified will be mitigated;
> i) the governance system the deployer will put in place, including human oversight, complaint-handling and redress.

### 4.1.5. General purpose AI systems

General purpose AI systems are defined[128] as any AI system that "*irrespective of how it is placed on the market or put into service, including as open source software - is intended by the provider to perform generally applicable functions such as image and speech recognition, audio and video generation, pattern detection, question answering, translation and others; a general purpose AI system may be used in a plurality of contexts and be integrated in a plurality of other AI systems".* Depending on how the HEROES tools are commercialised and exploited the provisions pertaining to general purposes AI systems might be applicable to HEROES technical partners.

Articles 4 (b) and 4 (c) provide general rules for general purpose AI systems and state that general purpose AI systems which may be used as high-risk AI systems or as components of high-risk AI systems (as per Art. 6) must comply with Title III, Chapter 2 requirements (requirements for high-risk AI systems). Nevertheless, the specific rules to be applied to general purpose systems will be governed by one or various implementing acts from the EC which will supplement the AI Act. Those implementing acts shall specify and adapt the application of the Title III, Chapter 2 requirements to general purpose AI systems and shall be enforceable no later than 18 months after the entry into force of the AI Act. Point 2 of Article 4 specifically stats that providers of general purpose AI systems shall comply, as from the date of application of the implementing acts, with the following **obligations**:

- Art. 16aa: indicate their name, registered trade name or registered trade mark, the address at which they can be contacted on the high-risk AI system or, where that is not possible, on its packaging or its accompanying documentation, as applicable;
- Art. 16e: ensure that the high-risk AI system undergoes the relevant conformity assessment procedure as referred to in Article 43, prior to its placing on the market or putting into service;
- Art. 16f: comply with the registration obligations referred to in Article 51(1);Art. 16g ('Obligations of providers of high-risk AI systems;
- Art. 16i: to affix the CE marking to their high-risk AI systems to indicate the conformity with this Regulation in accordance with Article 49;
- Art. 16j: upon request of a national competent authority, demonstrate the conformity of the highrisk AI system with the requirements set out in Chapter 2 of this Title;
- Art. 25: appointment of authorised representatives;
- Art. 48: EU declaration of conformity;
- Art. 61: Post-market monitoring by providers and post-market monitoring plan for high-risk AI systems.

Providers of general purpose AI systems shall cooperate and provide the necessary information to other providers that will put into service that system or will use it as a component of high-risk systems to enable them to comply with the Act. The provision of information shall not diminish jeopardise any intellectual property rights or confidential information.

Pursuant to Article 4 (c), the obligations pertaining to high-risk AI systems shall not apply to general purpose AI systems when the **provider has explicitly excluded all high-risk uses** in the instruction of use or information accompanying the general purpose AI system. Such exclusion must be made in *good faith* and shall *not be deemed justified if* the provider has sufficient reasons to consider that the system may be misused.

[128] Article 3 (1b) AI Act – Council's version.

 

When the provider detects or is informed about market misuse, they *shall take all necessary and proportionate measures to prevent* such further misuse, in particular taking into account the scale of the misuse and the seriousness of the associated risks.

### 4.1.6. Foundation models

A foundation models are defined in the AI Act[129] as an "*AI model that is trained on broad data at scale, is designed for generality of output, and can be adapted to a wide range of distinctive tasks*". This definition and concept is rather similar to how 'general purpose' AI systems are defined (see previous section) insofar as the main characteristic of both definitions is that both cover AI systems which can be adapted to perform a wide range of different functions. The difference seems to focus on the idea that foundation models are trained using vast amounts of 'broad' data, such as ChatGPT, however, one may wonder what threshold should be applied when considering that an AI system has been trained using large scale of data which is broad, since usually all AI systems are trained using datasets that contained data large scale data. Given that, foundation models will need to adhere to stricter rules on the AI Act, the material scope of foundation models will need to be clarified before the entry into force of the AI Act, otherwise there could be confusion and legal uncertainty around this point.

The new added Article 28 (b) regulates the obligations that providers of foundation models will be subject to prior to placing the system on the market or putting it into service, regardless of the AI system being provided as a service for payment, for free or under open-source licenses:

- Demonstrate that a risk assessment exercise has been carried out during and prior the development process even with the involvement of independent experts and that non-mitigable risks have been documented. This is similar to the risk management obligation of Article 9.
- Rely on datasets that are appropriate, suitable, and subject to governance measures, including the mitigation of possible biases. This obligation seems to be a 'soft' version of Article 10.
- Design and develop the model in order to achieve appropriate levels of performance, predictability, interpretability, corrigibility, safety and cybersecurity. Similar to the obligation provided by Article 15.
- Make use of applicable standards to reduce energy consumption, also enshrined in Article 12.
- Draw extensive technical documentation and instructions for use, in the same line as Article 11.
- Establish a quality management system, in line with Article 17.
- Register the model in the EU database, same obligation contained in Article 51 for high-risk AI systems.

In addition, those foundation models intended to generate with certain levels of autonomy, text, images, auditio or video (generative AI) shall also:

- Comply with transparency obligations outlined in Article 52.
- Generate the content in such a way to ensure compliance with applicable law, including intellectual property law, without prejudice to other fundamental rights, including freedom of expression.
- Document and make publicly available a summary on the use of training data protected under copyright.

[129] Article 3 (1c) added by the EP's text

In this regard, the regime designed for providers of foundation models seem to try to approximate the regime for high-risk AI systems in a 'soft' manner. This regime is becoming a point of disagreement in the AI Act discussions, with the latest reports suggesting that some EU countries, namely France, Germany, and Italy, have 'asked to retract the approach for foundation models', arguing that EU companies would lose competitiveness compared to US and Chinse Competitors[130]

## 4.2. AI standards

The current draft of the AI Act delegates to a great extent its technical provisions to standards, making reference to Regulation 1025/2015 on European Standardisation which allows the EC to request European standardisation organisations to draft standards for goods and services to be circulated within the EU. Article 40 of the AI Act states that the EC shall issue standardisation requests covering all requirements of the AI Act no later than 2 months after its entry into force. Nonetheless, the EC in 2022[131] issued a draft standardisation request to CEN and CENELEC (the European standards bodies) to create standards in support of safe and trustworthy AI in accordance with the High-Level Expert Group on AI principles. The list of requested standards as per Annex I comprehends the below list; and the initial stated deadline for adoption by CEN and CENELEC is the 31st of January 2025:

1- Risk management system for AI systems
2- Governance and quality of datasets used to build AI systems
3- Record keeping thorough logging capabilities by AI systems
4- Transparency and information provisions to the users of AI systems
5- Human oversight of AI systems
6- Accuracy specifications for AI systems
7- Robustness specifications for AI systems
8- Cybersecurity specifications for AI systems
9- Quality management system for providers of AI systems including post-marketing monitoring process
10- Conformity assessments for AI systems

In addition to EU standards, other international bodies such as the International Organisation for Standardisation ("**ISO**") have been working on the drafting and approval of AI standards, some of the current initiatives are included in the following table, we have selected those that might be relevant to the HEROES tools and technical partners[132]:

[130] EU's AI Act negotiations hit the brakes over foundation models, EURACTIV, Nov 203: https://www.euractiv.com/section/artificial-intelligence/news/eus-ai-act-negotiations-hit-the-brakes-over-foundation-models/
[131] Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence: https://ec.europa.eu/docsroom/documents/52376
[132] Report on the Core Principles and Opportunities for Responsible and Trustworthy AI: https://iuk.ktn-uk.org/wp-content/uploads/2023/10/responsible-trustworthy-ai-report.pdf

 

*Table 1: Draft and published standards regulating AI systems*

| Publisher | Code | Standard name | Development stage |
|---|---|---|---|
| **ISO/IEC** | WD 12792 | Information technology — Artificial intelligence — Transparency taxonomy of AI systems | Draft |
| **ISO/IEC** | WD TS 5471 | Information technology — Artificial intelligence (AI) — Quality evaluation guidelines for AI systems | Draft |
| **IEE** | P2976 | Standard for XAI – eXplainable Artificial Intelligence – for Achieving Clarity and Interoperability of AI Systems Design | Draft |
| **ISO/IEC** | AWI TS 6254 | Objectives and approaches for explainability of ML models and AI systems | Draft |
| **ISO/IEC** | DIS 25059 | Information technology — Software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Quality model for AI systems | Draft |
| **CSA** | CAN/CI OSC 101 | Ethical design and use of automated decision systems | Published |
| **ISO/IEC** | AWI TR 5469 | Overview of trustworthiness in artificial intelligence | Published |
| **IEEE** | P2945 | Standard for Technical Requirements for Face Recognition Systems | Draft |
| **IEEE** | P3129 | Standard for Robustness Testing and Evaluation of Artificial Intelligence (AI)-based Image Recognition Service | Draft |
| **ISO/IEC** | TR 2911911 | Software and systems engineering – Software testing – Part 11: Guidelines on the testing of AI-based systems | Published |
| **ISO/IEC** | TR 24029- 1 | Artificial Intelligence (AI) – Assessment of the robustness of neural networks – Part 1: Overview | Published |
| **ISO/IEC** | TR 24029- 1 | Artificial intelligence (AI) — Assessment of the robustness of neural networks — Part 2: Methodology for the use of formal methods | Published |
| **ISO/IEC** | 23894 | Information technology – Artificial intelligence – Risk management | Published |
| **ISO/IEC** | AWI TS 20119-11 | Information technology — Artificial intelligence — Testing for AI systems — Part 11 | Published |
| **ISO/IEC** | TR 24027 | Information technology – Artificial intelligence (AI) – Bias in AI systems and AI aided decision making | Published |
| **ISO/IEC** | TS 3805-3 | Information technology. Governance of data. Guidelines for data classification | Published |
| **IEEE** | 3652.1 | IEEE Guide for Architectural Framework and Application of Federated Machine Learning | Published |

| | | | |
|---|---|---|---|
| **ISO/IEC** | DIS 42001 | Information technology — Artificial intelligence — Management system | Draft |
| **ISO/IEC** | FDIS 24668 | Information technology — Artificial intelligence (AI) — Process management framework for big data analytics | Draft |
| **ISO/IEC** | 24368 | Information technology — Artificial intelligence — Overview of ethical and societal concerns | Published |
| **ISO/IEC** | DTS 4213 | Information technology — Artificial intelligence (AI) — Assessment of machine learning classification performance | |
| **IEE** | P3123 | Standard for Artificial Intelligence and Machine Learning (AI/ML) Terminology and Data Formats | Draft |
| **ISO/IEC** | DIS 8183 | Information technology — Artificial intelligence — Data life cycle framework | Draft |
| **ISO/IEC** | AWI 5259-2 | Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures | Draft |
| **ISO/IEC** | AWI 5259-1 | Artificial intelligence — Data quality for analytics and machine learning (ML) — Part 2: Data quality measures | Draft |

## 4.3. Council of Europe's initiative for an international convention on AI

In 2020, the Parliament Assembly of the Council of Europe adopted the Resolution 2341 (2020) on the "*Need for democratic governance of artificial intelligence*". The Resolution notes that "*in recent years, governments, civil society, international institutions and companies have been engaged in extensive discussions with a view to identifying a set of commonly accepted principles on hot respond to concerns related to AI use*" and considers that 'self-regulatory ethical principles and policies voluntarily introduced by private actors are inadequate and insufficient tools to regulate AI as they do not necessarily lead to democratic oversight and accountability". In this Resolution, the Council mandates the Ad-hoc Committee on AI to examine the potential elements to be included in a legal framework for the design, development and application of AI that would guarantee AI compliance with human rights, democracy, and the rule of law.

In January 2023, the Committee on AI published a zero draft for a Convention on AI, Human Rights and the Rule of Law[133] and in July a consolidated draft. The latest draft consists of 34 articles divided in eight chapters. Chapter III, identifies six principles applicable to the design, development, and application of AI:

- Principle of equality and anti-discrimination
- Principle of privacy and personal data protection
- Principle of accountability, responsibility, and legal liability
- Principle of transparency and oversight
- Principle of safety
- Principle of safe innovation

[133] Revised Zero Draft [Framework] Convention on AI, Human Rights and the Rule of Law, January 2023: https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f

 

Chapter I of the Convention, similarly to the draft on the AI Act, sets out a risk-based approach, mandating its signatory parties to implement 'graduated' and 'differentiated' measures ruling the entire AI systems' lifecycle in its domestic legal systems governing AI systems in accordance with the severity and potential threats of AI systems to "*human rights and fundamental freedoms, democracy and the rule of law during design, development, use and decommissioning of artificial intelligence systems*"[134].

Chapter IV mandates the introduction of national legislation that would protect individuals against violations of human rights and fundamental freedoms resulting for the use of AI systems along with appropriate remedies and the requirement for the AI system to record its uses so that affected individuals could contest any of its decisions. This establishes links with the proposed AI liability directive at the EU level, which goes beyond these requirements by introducing a provision that would alleviate the burden of proof for victims of AI system by introducing a 'presumption of causality' if it can be proven that there was a lack of compliance with a certain obligation and that there is a link with this non-compliance and the harm caused. The procedural safeguards set out in Article 14 state that natural persons shall have the right to know that they are interacting with an AI system rather than a human being. Arguably a procedural safeguard, this obligation could be seen as a transparency obligation in line with the current draft of the AI Act which provides for the same in its Article 52.

Chapter V caters for the assessment and mitigation of risks and adverse impacts to human rights, democracy, and the rule of law. The Convention would mandate to implement the obligation of producing risk management systems throughout the lifecycle of the AI system in accordance with the risk posed and potential threats.

The Convention dedicates one article to the protection of children. Article 18 states that the signatory parties will need to "*take due account of any specific needs and vulnerabilities in relation to the respect of the rights of persons with disabilities and of children*". This provision comes in a political and social context where there is a growing discussion on the unsupervised use of social networks by minors and its negative consequences, along with growing regulatory initiatives at EU and national level to incorporate mechanisms for age verification to pornographic sites, the banning of behavioural publicity targeting of children, where it can be argued that the protection of children is in the spotlight of policymakers and regulators in a transversal way. It is nonetheless surprising that the current draft of the Convention only dedicates only one Article as a general reference to the protection of minors. On the contrary, the draft of the AI Act specifically lists as one of the requirements on performing risk assessments and implementing a risk management system to consider the risks that may adversely impact vulnerable groups and children, creating an obligation to specifically consider these risks and mitigate them before placing the system in the market or putting it to service and potentially cause any harm on children.

Even if the Convention aims at making AI systems to comply with human rights, democracy and the rule of law and the initiatives for self-regulation advocated by private companies have been deemed by the Council inadequate and insufficient, ironically, all civil society organisations, such as AlgorithmicWatch, Fair Trials, or Homo Digitalis, were excluded from the drafting process of the Convention that would be the first international treaty on AI. Allegedly, this exclusion was due to the request of the US to avoid countries' positions becoming public,[135] presumably since the US has been advocating for the scope of the treaty to cover only public bodies and leaving out private companies "in which American companies play a world-leading role"[136]. Even if some countries asked for the participation of civil society organisations, this first draft was released without them. In subsequent versions and discussions, they will be included, but NGOs fear that by then their position will be easily neglected.

[134] Article 2 of the consolidated draft of the Convention
[135] Euractiv Jan 23, US obtains exclusion of NGOs from drafting AI treaty: https://www.euractiv.com/section/digital/news/us-obtains-exclusion-of-ngos-from-drafting-ai-treaty/
[136] Ibid

The zero-draft released by the Committee included a specific chapter on the obligations for public authorities but also specific provisions binding for private actors, however the text might suffer substantial amendments until its final approval. In addition, the identified principles would apply to both. According to EURACTIV, the EC which would be entitled to negotiate on behalf of the 27 EU members is trying to hold its position until there has been further progress on the regulation of the AI Act.

In July 23, a consolidated working draft of the Convention was published[137] where references to obligations solely pertaining to public authorities have been removed, hence the scope of the Convention and its obligations would apply to public and private actors equally. In a similar was as provided by the current draft of the AI Act, research and development activities regarding AI will be left out of the scope of both frameworks unless they are tested or otherwise used in ways that have the potential to interfere with human rights, democracy and the rule of law.

[137] Consolidated draft, Convention on AI, Council of Europe, July 23: https://rm.coe.int/cai-2023-18-consolidated-working-draft-framework-convention/1680abde66

 

# Conclusions

We have explored the law that is relevant to LEAs in collecting electronic evidence, to the management of data by network operators, and to technology developers working on tools for combating THB and CSA/E. The relevant law is developing rapidly. Several key instruments are well-developed and have undergone a high degree of scrutiny, most notably, the EU AI Act. Other key instruments, such as the DSA, have been agreed but not implemented, or have only very recently been implemented, and have not yet undergone the scrutiny of appellate and higher courts. The general picture, then, is that there is a degree of uncertainty, but that it is clear that a new regime is being established.

There are two key themes in the development of this new regime.

- First, there is a tendency to defer one of the fundamental issues that legislation in this area must face, namely, the problems of confronting security and safety with privacy. As we saw, many of the specifics in the EU AI Act are to be delegated to the work of standards bodies, and furthermore, the precise implications of the UK Online Safety Act for the extent of service provider data collection obligations remain unclear, even after the Act's passing.
- Second, there is also a tendency to skirt around the problems of international relations as they relate to e-evidence and data transfer. Treaties on e-evidence are, remarkably, referred to by the parties as 'agreements' and, rather than taking a principled approach, have thus far been negotiated in a piecemeal manner that is subjected to the power differentials of the parties. Relatedly, we have seen a reluctance to involve civil society organisations expertise in the development of the AI Act.

It is in one way understandable that legislators defer the difficult questions, and it may be the case that a more cautiously developed legal regime will be a better one. Nonetheless, LEAs, ISPs and technology developers should expect unclarity for some time to come.

# References


1. E-Privacy Regulation Proposal:

   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010

2. Council of the EU, February 2021, amendments and new text draft, AI Act:

   https://data.consilium.europa.eu/doc/document/ST-6087-2021-INIT/en/pdf

3. Context of the e-Privacy Regulation Proposal, point 1.2:

   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017PC0010

4. Regulation 2021/1232 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse:
   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R1232

5. Regulation laying down rules to prevent and combat child sexual abuse‘ (2022/0155(COD)) (2022):
   https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN

6. Online Safety Act UK:
   https://www.legislation.gov.uk/ukpga/2023/50/enacted

7. Department for Science, Innovation and Technology and The Rt Hon Michelle Donelan MP, ‘Britain makes internet safer, as Online Safety Bill finished and ready to become law’, *GOV.UK*, (2023):
   https://www.gov.uk/government/news/britain-makes-internet-safer-as-online-safety-bill-finished-and-ready-to-become-law.

8. HM Government, ‘Government response to the Internet Safety Strategy Green Paper’, *GOV.UK*, (2018):
   https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper#full-publication-update-history

9. Amnesty International, ‘UK: ‘Spy clause’ in Online Safety Bill must be addressed before it becomes law’, (5th September 2023):
   https://www.amnesty.org.uk/press-releases/uk-spy-clause-online-safety-bill-could-lead-mass-surveillance

10. Department for Culture, Media & Sport, Home Office, and Department for Digital, Culture, Media & Sport, ‘Interim code of practice on online child sexual exploitation and abuse’, *GOV.UK*, (2020):
    https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice

11. John Woodhouse, Sally Lipscombe and Lorraine Conway, ‘Analysis of the Online Safety Bill’, *House of Commons Library*, (2022):
    https://commonslibrary.parliament.uk/research-briefings/cbp-9506/

12. Department for Digital, Culture, Media & Sport and Home Office, ‘Online Harms White Paper’, *GOV.UK*, (8th April 2019):
    https://www.gov.uk/government/consultations/online-harms-white-paper

13. National Crime Agency, ‘New reporting regime for online child sexual abuse content announced’, (17th March 2022):
    https://www.nationalcrimeagency.gov.uk/news/new-reporting-regime-for-online-child-sexual-abuse-content-announced


 

14. Parliamentary Briefing: Report Stage of the Online Safety Bill', (July 2022): https://www.nspcc.org.uk/globalassets/documents/policy/online-safety-bill-report-stage-parliamentary-briefing.pdf

15. Ian Levy and Crispin Robinson, 'Thoughts on child safety on commodity platforms', *arXiv*, (2022): https://doi.org/10.48550/arXiv.2207.09506.

16. NSPCC, 'Online Safety Bill Briefing: Consideration of Lords Amendments – House of Commons', (September 2023): https://www.nspcc.org.uk/globalassets/documents/online-safety/nspcc-online-safety-bill-brief---sept-23.pdf

17. NSPCC, 'Public backs action to prevent child abuse in private messaging', (5th July 2023): https://www.nspcc.org.uk/about-us/news-opinion/2023/Public-backs-action-to-prevent-child-abuse-in-private-messaging/

18. Benjamin Dowling, 'The UK just passed an online safety law that could make people less safe', *The Conversation*, (25th September 2023): https://theconversation.com/the-uk-just-passed-an-online-safety-law-that-could-make-people-less-safe-213595

19. Matthew Hodgson et al., 'An open letter', *WhatsApp Blog*, (17th April 2023): https://blog.whatsapp.com/an-open-letter?lang=en

20. National Crime Agency, 'Global law enforcement coalition urges tech companies to rethink encryption plan that put children in danger from online abusers', 19th April 2023, https://www.nationalcrimeagency.gov.uk/news/global-law-enforcement-coalition-urges-tech-companies-to-rethink-encryption-plans-that-put-children-in-danger-from-online-abusers

21. Department for Digital, Culture, Media & Sport and Department for Science, Innovation & Technology, 'Government response to the Joint Committee report on the draft Online Safety Bill', *GOV.UK*, (17th March 2022): https://www.gov.uk/government/publications/joint-committee-report-on-the-draft-online-safety-bill-government-response/government-response-to-the-joint-committee-report-on-the-draft-online-safety-bill

22. NSPCC, 'We're calling for effective action in the Online Safety Bill as child abuse image crimes reach record level', (22nd February 2023): https://www.nspcc.org.uk/about-us/news-opinion/2023/2023-02-22-were-calling-for-effective-action-in-the-online-safety-bill-as-child-abuse-image-crimes-reach-record-levels/

23. Martin Albrecht and Hamed Haddadi et al, 'Open Letter from Security and Privacy Researchers in relation to the Online Safety Bill': https://haddadi.github.io/UKOSBOpenletter.pdf

24. The Chartered Institute for IT, 'The Online Safety Bill and the role of technology in child protection', (31st August 2023): https://www.bcs.org/media/10993/online-safety-bill-and-the-role-of-technology-in-child-protection.pdf.

25. HL Deb 6 September 2023, vol 832, col 458. Available at: https://hansard.parliament.uk/lords/2023-09-06/debates/4AC6A32E-0C53-46C7-A714-AD4165C484D7/OnlineSafetyBill

26. Ofcom, 'Ofcom's approach to implementing the Online Safety Act', (26th October 2023): https://www.ofcom.org.uk/online-safety/information-for-industry/roadmap-to-regulation.

27. European Commission, press release April 2018, FAQs: New rules to obtain electronic evidence: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

28. The Purpose and Impact of the CLOUD Act - FAQs: https://www.justice.gov/criminal-oia/page/file/1153466/download

29. Council Decision (EU) 2016/920 of 20 May 2016 on the signing, on behalf of the European Union, of the Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016D0920

30. Agreement between the US and the EU on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A22016A1210%2801%29

31. Jessica Shurson, Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law, International Journal of Law and Information Technology, 2020:

32. Eur lex summary of EU-US agreement on personal data protection: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3A3104_8

33. Regulation (Eu) 2023/1543 of the European Parliament and of the Council of 12 of July 2023 on European Production Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings:

    https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543

34. EC, March 23, EU-U.S. announcement on the resumption of negotiations on an EU-U.S. agreement to facilitate access to electronic evidence in criminal investigations: https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en

35. Council of the EU, Feb 2019, Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters:

    https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019PC0070

36. UK – US Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime: https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019

37. UK Parliament, Roadmap UK-US Agreement:

    https://api.parliament.uk/view/treaty/bjKV1oDq

38. Office of public affairs U.S Department of Justice, Landmark US-UK Data Access Agreement Enters into Force:

    https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force

39. The Clarifying Lawful Overseas use of Data or CLOUD Act:

    https://www.congress.gov/bill/115th-congress/senate-bill/2383/text#:~:text=3)%20the%20agreement,the%20United%20States%3B

40. The globalisation of criminal evidence and the UK-US Data Sharing Agreement, BLC partners Michael Drury and Julian Hayes, M arch 2022:

 

https://www.bcl.com/the-globalisation-of-criminal-evidence-and-the-uk-us-data-sharing-agreement/

41. Australia-US CLOUD Act Agreement:

    https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/australia-united-states-cloud-act-agreement#:~:text=The%20Australia%2DUS%20CLOUD%20Act%20Agreement%20is%20focussed%20on%20allowing,located%20in%20their%20own%20jurisdiction. Link to the Agreement: https://www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf

42. Australia, Telecommunication Legislation Amendment (International Production Orders) Bill: https://parlwork.aph.gov.au/Bills/r6511

43. Parliamentary Question: UK-US agreement under the US CLOUD Act, Oct 2019: https://www.europarl.europa.eu/doceo/document/E-9-2019-003136_EN.html

44. Ethics guidelines for trustworthy AI, EC 2029:

    https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

45. EC proposal for an AI Regulation:

    https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

46. AI Act Proposal, version of the EU Council, December 2021: https://data.consilium.europa.eu/doc/document/ST-15698-2022-INIT/EN/pdf

47. Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence:

    https://ec.europa.eu/docsroom/documents/52376

48. Report on the Core Principles and Opportunities for Responsible and Trustworthy AI:

    https://iuk.ktn-uk.org/wp-content/uploads/2023/10/responsible-trustworthy-ai-report.pdf

49. Revised Zero Draft [Framework] Convention on AI, Human Rights and the Rule of Law, January 2023:

    https://rm.coe.int/cai-2023-01-revised-zero-draft-framework-convention-public/1680aa193f

50. Euractiv Jan 23, US obtains exclusion of NGOs from drafting AI treaty: https://www.euractiv.com/section/digital/news/us-obtains-exclusion-of-ngos-from-drafting-ai-treaty/

51. Consolidated Working Draft of the Framework Convention on AI, Human Rights, Democracy and the Rule of Law, Council of Europe, July 23:

    https://rm.coe.int/cai-2023-18-consolidated-working-draft-framework-convention/1680abde66

52. European Commission, Q&As: AI Liability Directive:

    www.ec.europa.eu/commission/presscorner/detail/en/qanda_22_5793

53. EU's AI Act negotiations hit the brakes over foundation models, EURACTIV, Nov 203: https://www.euractiv.com/section/artificial-intelligence/news/eus-ai-act-negotiations-hit-the-brakes-over-foundation-models/

54. EURACTIV October 23, EU Parliament nails down agreement on child sexual abuse regulation: https://www.euractiv.com/section/law-enforcement/news/eu-parliament-nails-down-agreement-on-child-sexual-abuse-regulation/

55. MEPs reach political agreement to protect children and privacy: https://iptegrity.com/index.php/european-union/privacy/1160-european-parliament-tables-pragmatic-proposal-to-protect-children-on-line