

Πρόγραμμα Μεταπτυχιακών Σπουδών

# Διαχείριση και Ανάδειξη Πολιτιστικής Πληροφορίας

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ - Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας &amp; Μουσειολογίας

[Διαχείριση και Ανάδειξη Πολιτιστικής Πληροφορίας](#): Δίκαιο και Δεοντολογία Πολιτιστικής Πληροφορίας (Υ)

Αρχική Πρόγραμμα  
Σπουδών ΣυνεργάτεςΕπιστημονικές  
Δημοσιεύσεις-  
Διπλωματικές  
ΕργασίεςΩρολόγιο  
ΠρόγραμμαΠροκήρυξη  
ΠΜΣΑκαδημαϊκή  
Δεοντολογία και  
Ακαδημαϊκοί  
Σύμβουλοι

Έγγραφα-Κανονισμοί ▾

Ανακοινώσεις-  
Ενημέρωση  
Ερευνητικών  
ΔραστηριοτήτωνΥποδομές  
και Χρήσιμοι  
Σύνδεσμοι

## Διαχείριση Ψηφιακής Πληροφορίας - Υπηρεσίες Πληροφόρησης

Πρόγραμμα Μεταπτυχιακών Σπουδών, Τμήμα Αρχειονομίας, Βιβλιοθηκονομίας και Μουσειολογίας, Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής,  
Ιόνιο Πανεπιστήμιο

[Διαχείριση Ψηφιακής Πληροφορίας - Υπηρεσίες Πληροφόρησης](#): Δίκαιο Πληροφορίας (Ε)

Γιώργος Μπουχάγιαρ  
Vrije Universiteit Brussel (Free University of Brussels)  
Ιόνιο Πανεπιστήμιο

Email: [georgios.bouchagiar@vub.be](mailto:georgios.bouchagiar@vub.be) & [georgebouchayar@ionio.gr](mailto:georgebouchayar@ionio.gr)

# Προτάσεις για παρουσιάσεις



[DE - EN - ES - FR - IT]

DICASTERY FOR THE DOCTRINE OF THE FAITH  
DICASTERY FOR CULTURE AND EDUCATION

## ANTIQUA ET NOVA

### **Note on the Relationship Between Artificial Intelligence and Human Intelligence**

#### **I. Introduction**

1. With wisdom both ancient and new (cf. Mt. 13:52), we are called to reflect on the current challenges and opportunities posed by scientific and technological advancements, particularly by the recent development of Artificial Intelligence (AI). The Christian tradition regards the gift of intelligence as an essential aspect of how humans are created “in the image of God” (Gen. 1:27). Starting from an integral vision of the human person and the biblical calling to “till” and “keep” the earth (Gen. 2:15), the Church emphasizes that this gift of intelligence should be expressed through the responsible use of reason and technical abilities in the stewardship of the created world.

2. The Church encourages the advancement of science, technology, the arts, and other forms of human endeavor, viewing them as part of the “collaboration of man and woman with God in perfecting the visible creation.”<sup>[1]</sup> As Sirach affirms, God “gave skill to human beings, that he might be glorified in his marvelous works” (Sir. 38:6). Human abilities and creativity come from God and, when used rightly, glorify God by reflecting his wisdom and goodness. In light of this, when we ask ourselves what it means to “be human,” we cannot exclude a consideration of our scientific and technological abilities.

3. It is within this perspective that the present *Note* addresses the anthropological and ethical challenges raised by AI—issues that are particularly significant, as one of the goals of this technology is *to imitate the human intelligence that designed it*. For instance, unlike many other human creations, AI can be trained on the results of human creativity and then generate new “artifacts” with a level of speed and skill that often rivals or surpasses what humans can do, such as producing text or images indistinguishable from human compositions. This raises critical concerns about AI’s potential role in the growing crisis of truth in the public forum. Moreover, this technology is designed to learn and make certain choices autonomously, adapting to new situations and providing solutions not foreseen by its programmers, and thus, it raises fundamental questions about ethical responsibility and human safety, with broader implications for society as a whole. This new situation has prompted many people to reflect on what it means to be human and the role of humanity in the world.

## China's Approach to AI Anthropomorphism

China's proposed AI law acknowledges AI-related human vulnerabilities and establishes contextual technical measures to prevent AI harms | Edition #264



LUIZA JAROVSKY, PHD  
JAN 13, 2026

👍 147

💬 18

🔄 42

Share



<https://www.luizasnewsletter.com/p/chinas-approach-to-ai-anthropomorphism>

[Home](#) | [Updates](#) | China sets trial ethics rules for AI science and technology activities

13 Apr 2026

## China sets trial ethics rules for AI science and technology activities

*New trial rules in China set out ethics review procedures for AI science and technology activities.*



<https://dig.watch/updates/china-ai-science-technology-ethics-review>



[Home](#) | [Updates](#) | China sets trial ethics rules for AI science and technology activities

Local authorities and relevant departments may also establish specialised ethics review and service centres that provide review, re-examination, training, and consulting services on commission, but may not both review and re-examine the same AI activity.

The text sets out application and review procedures, including general, simplified, expert re-examination, and emergency procedures. It says review should focus on human well-being, fairness and justice, controllability and trustworthiness, transparency and explainability, traceability of responsibility, and privacy protection. **Review decisions are to be made within 30 days after acceptance, subject to extension in complex cases. An emergency review is generally completed within 72 hours.**

The measures also provide for expert re-examination of listed activities. The attached list covers human-machine integrated systems with a strong influence on human behaviour, psychological emotions, or health; algorithmic models, applications, and systems with the capacity for social mobilisation or guidance of social consciousness; and highly autonomous automated decision systems used in scenarios involving safety or health risks. The text says the list will be adjusted dynamically as needed.

The document further states that violations may be investigated and handled under laws, including the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and the Science and Technology Progress Law. According to the text, the measures take effect upon issuance.



2f59

1 / 71 | - 100% + | [Print] [Refresh] [Zoom] [Back] [Forward]



- 1
- 2
- 3



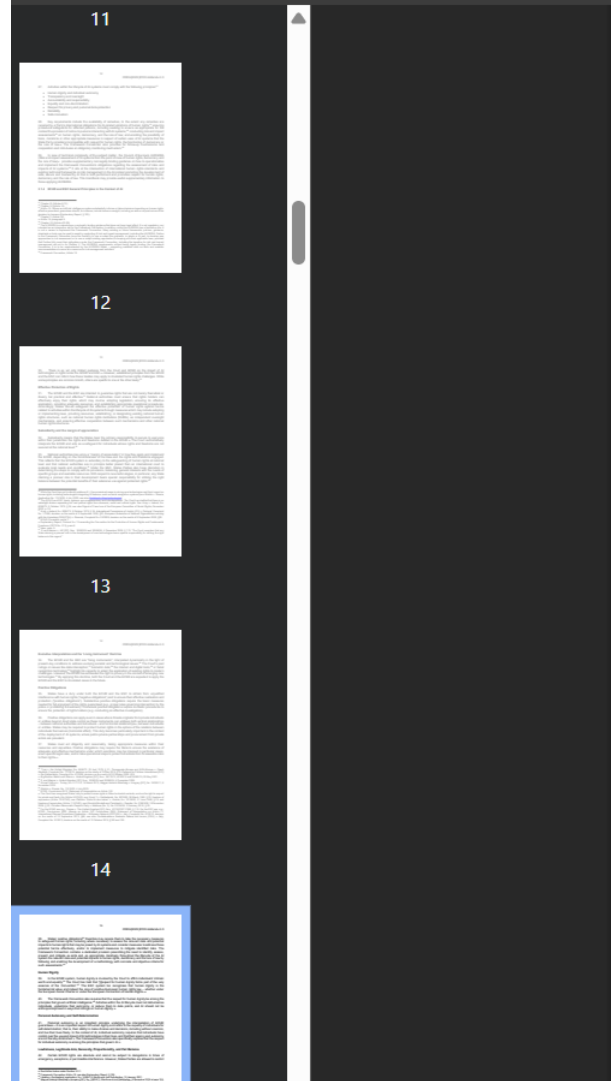
CDDH(2025)R103 Addendum 3  
12 January 2026

## STEERING COMMITTEE FOR HUMAN RIGHTS

(CDDH)

### CDDH HANDBOOK ON HUMAN RIGHTS AND ARTIFICIAL INTELLIGENCE

<https://rm.coe.int/steering-committee-for-human-rights-cddh-cddh-handbook-on-human-rights/48802a2f59>



38. States' positive obligations<sup>64</sup> therefore may require them to take the necessary measures to safeguard human rights, including where necessary to assess the relevant risks and potential impacts to human rights that may be posed by AI systems and consider measures to address those potential harms effectively, and/or to implement measures to mitigate identified risks. The Framework Convention contains a dedicated provision prescribing the need to identify, assess, prevent and mitigate *ex ante* and, as appropriate, iteratively throughout the lifecycle of the AI system the relevant risks and potential impacts to human rights, democracy and the rule of law by following and enabling the development of a methodology with concrete and objective criteria for such assessments.<sup>65</sup>

**Human Dignity**

39. In the ECHR system, human dignity is invoked by the Court to affirm individuals' intrinsic worth and equality.<sup>66</sup> The Court has held that "[r]espect for human dignity forms part of the very essence of the Convention".<sup>67</sup> The ESC system too recognises that human dignity is the fundamental value and indeed the core of positive European human rights law – whether under the European Social Charter or under the European Convention of Human Rights.<sup>68</sup>

40. The Framework Convention also requires that the respect for human dignity be among the principles that govern artificial intelligence.<sup>69</sup> Activities within the AI lifecycle must not dehumanise individuals, undermine their autonomy, or reduce them to data points, and AI should not be anthropomorphised in ways that infringe on human dignity.<sup>70</sup>

**Personal Autonomy and Self-Determination**

41. Personal autonomy is an important principle underlying the interpretation of ECHR guarantees.<sup>71</sup> It is an important aspect of human dignity and refers to the capacity of individuals for self-determination; that is, their ability to make choices and decisions, including without coercion, and live their lives freely. In the context of AI, individual autonomy requires that individuals have control over the use and impact of AI technologies in their lives, and that their agency and autonomy are not thereby diminished.<sup>72</sup> The Framework Convention also specifically requires that the respect for individual autonomy is among the principles that govern AI.<sup>73</sup>

**Lawfulness, Legitimate Aim, Necessity, Proportionality, and Fair Balance**

42. Certain ECHR rights are absolute and cannot be subject to derogations in times of emergency, exceptions, or permissible interference. However, States Parties are allowed to restrict



IMAGE CREDITS: OLIVIER MORIN/AFP / GETTY IMAGES

AI



# Florida AG announces investigation into OpenAI over shooting that allegedly involved ChatGPT

Lucas Ropek — 1:11 PM PDT · April 9, 2026

Florida's attorney general, James Uthmeier, announced Thursday that his office planned to investigate OpenAI over the alleged role of ChatGPT in a deadly shooting last year.



<https://techcrunch.com/2026/04/09/florida-ag-investigation-openai-chatgpt-shooting/>

OPINION

# Why having “humans in the loop” in an AI war is an illusion

We don't really understand AI's inner workings, so we're effectively flying blind.

By Uri Maoz

April 16, 2026



[https://www.technologyreview.com/2026/04/16/1136029/humans-in-the-loop-ai-war-illusion/?utm\\_source=LinkedIn&utm\\_campaign=site\\_visitor.unpaid.engagement&utm\\_medium=tr\\_social](https://www.technologyreview.com/2026/04/16/1136029/humans-in-the-loop-ai-war-illusion/?utm_source=LinkedIn&utm_campaign=site_visitor.unpaid.engagement&utm_medium=tr_social)

🔍 Search for articles...

All Collections > Safeguards > Identity verification on Claude

## Identity verification on Claude

Updated this week

Being responsible with powerful technology starts with knowing who is using it. Identity verification helps us prevent abuse, enforce our usage policies, and comply with legal obligations.

We are rolling out identity verification for a few use cases, and you might see a verification prompt when accessing certain capabilities, as part of our routine platform integrity checks, or other safety and compliance measures.

We only use your verification data to confirm who you are and not for any other purposes.

### How are we verifying?

We selected Persona Identities as our verification partner based on the strength of their technology, privacy controls, and security safeguards. Follow the steps below to complete your identity verification process.

How are we verifying?

What you'll need

Accepted ID types

How your data is protected

What we're not doing

What if my verification fails?

Why did my account get banned after verification?

Questions?



r/ClaudeCode • 1d ago  
Direct-Attention8597



## Anthropic just quietly launched ID verification for Claude, and the timing couldn't be more ironic

Anthropic rolled out government ID verification for Claude this week via a third-party service called Persona Identities. You may be asked to upload a physical government-issued photo ID (passport, driver's license, or national ID) plus a live selfie depending on the features you use.

Here's the official reasoning from Anthropic's help center: prevent abuse, enforce usage policies, and fulfill legal obligations. They also say the data won't be used for training, marketing, or advertising, only for identity confirmation.

### Why this is raising eyebrows:

A few months ago, millions of users migrated from ChatGPT to Claude specifically because Anthropic declined a Pentagon contract over concerns about mass surveillance and autonomous weapons. The privacy-focused positioning was a big part of Claude's appeal. Now those same users are being asked to hand over biometric data and government IDs.

### Some context that makes this more uncomfortable:

Persona, the verification partner Anthropic selected, had a documented data breach in late 2025 that exposed around 70,000 government ID images from Discord users. Separate investigations have also found that Persona may share user data with up to 17 sub-processors.

### What Anthropic says about data handling:

Verification data stays between you, Persona, and Anthropic. It won't be shared with third parties for marketing or unrelated purposes. Anthropic is the "data controller," meaning they set the rules for how it's used and retained.

### The rollout:

It's not hitting everyone at once. Right now it's being triggered for select use cases and certain users, with broader rollout coming gradually.

This is the first major AI chatbot to require this level of identity verification. No word yet on whether this will become a requirement for basic access or stay limited to specific features.

edit

e

er Platform

ro BETA

reddit

ules



Marshall McLuhan 1966 - Predicting the Internet with Robert Fulford

This Is Marshall McLuhan - The

Wednesday 15 April, 2026  
49m · 8

00:02:16 00:47:22

⏪ ⏩ 🔊 ⚙️ ⓘ 🗄️

JUSTICE DEPARTMENT

# DOJ recommends bringing back firing squads in federal executions

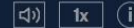
In a new report, the Justice Department noted the challenges of procuring the drugs needed for lethal injections.



Listen to this article with a [free account](#)

00:00

04:35



<https://www.nbcnews.com/politics/justice-department/trump-justice-department-firing-squads-lethal-injection-executions-rcna341897>





# School Readiness Survey

For the past six years, Kindred<sup>2</sup> has surveyed thousands of teachers and parents to source robust evidence of the proportion of children that are considered 'school ready', comparing this to perceptions of parents.

We use this school readiness evidence to highlight the impact on children and schools when pupils arrive in Reception having not met their developmental milestones and the difficulties that children, families and schools face from this.

## — 2025 School Readiness Survey

Our sixth annual school readiness report once again sets out perceptions of the scale and impact of children missing their early developmental milestones. The survey finds that the number of children who are 'school ready' has declined significantly since 2024.



# Τεχνητή Νοημοσύνη

**GDPR**

**AI Act**

# Τεχνητή Νοημοσύνη

**GDPR**



**DPIA**

**(Data Protection Impact Assessment)**

**AI Act**



**FRIA**

**(Fundamental Rights Impact Assessment)**

# Τεχνητή Νοημοσύνη

## GDPR



## DPIA

**(Data Protection Impact Assessment)**

*Άρθρο 35*

### Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.
2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.
3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:
  - α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,
  - β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή
  - γ) συστηματικής παρακολούθησης δημοσίας προσβάσιμου χώρου σε μεγάλη κλίμακα.

## AI Act



## FRIA

**(Fundamental Rights Impact Assessment)**

*Άρθρο 27*

### Εκτίμηση επιπτώσεων των συστημάτων ΤΝ υψηλού κινδύνου στα θεμελιώδη δικαιώματα

1. Πριν από την ανάπτυξη συστήματος ΤΝ υψηλού κινδύνου που αναφέρεται στο άρθρο 6 παράγραφος 2, με την εξαίρεση συστημάτων ΤΝ υψηλού κινδύνου που προορίζονται για χρήση στον τομέα που αναφέρεται στο παράρτημα ΙΙΙ σημείο 2, οι φορείς εφαρμογής που είναι οργανισμοί δημόσιου δικαίου ή ιδιωτικές οντότητες που παρέχουν δημόσιες υπηρεσίες και οι φορείς εφαρμογής συστημάτων ΤΝ υψηλού κινδύνου που αναφέρονται στο παράρτημα ΙΙΙ σημείο 5 στοιχεία β) και γ) διενεργούν εκτίμηση των επιπτώσεων που μπορεί να έχει στα θεμελιώδη δικαιώματα η χρήση του συστήματος. Για τον σκοπό αυτόν, οι φορείς εφαρμογής διενεργούν εκτίμηση που περιλαμβάνει:
  - α) περιγραφή των διαδικασιών του φορέα εφαρμογής στις οποίες το σύστημα ΤΝ υψηλού κινδύνου θα χρησιμοποιείται σύμφωνα με τον επιδιωκόμενο σκοπό του·
  - β) περιγραφή του χρονικού διαστήματος εντός του οποίου και της συχνότητας με την οποία προορίζεται να χρησιμοποιηθεί κάθε σύστημα ΤΝ υψηλού κινδύνου·
  - γ) τις κατηγορίες φυσικών προσώπων και ομάδων που είναι πιθανό να επηρεαστούν από τη χρήση του στο συγκεκριμένο πλαίσιο·
  - δ) τους συγκεκριμένους κινδύνους βλάβης που είναι πιθανό να επηρεάσουν τις κατηγορίες φυσικών προσώπων ή ομάδων προσώπων που προσδιορίζονται δυνάμει του στοιχείου γ) της παρούσας παραγράφου, λαμβανομένων υπόψη των πληροφοριών που δίνει ο πάροχος δυνάμει του άρθρου 13·
  - ε) περιγραφή της εφαρμογής των μέτρων ανθρώπινης εποπτείας, σύμφωνα με τις οδηγίες χρήσης·
  - στ) τα μέτρα που πρέπει να λαμβάνονται σε περίπτωση επέλευσης των εν λόγω κινδύνων, συμπεριλαμβανομένων των ρυθμίσεων για την εσωτερική διακυβέρνηση και τους μηχανισμούς υποβολής καταγγελιών.

# Τεχνητή Νοημοσύνη

## GDPR



## DPIA

**(Data Protection Impact Assessment)**

*Άρθρο 35*

### Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.
2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.
3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:
  - α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,
  - β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή
  - γ) συστηματικής παρακολούθησης δημοσίας προσβάσιμου χώρου σε μεγάλη κλίμακα.

## AI Act



## FRIA

**(Fundamental Rights Impact Assessment)**

*Άρθρο 27*

### Εκτίμηση επιπτώσεων των συστημάτων ΤΝ υψηλού κινδύνου στα θεμελιώδη δικαιώματα

1. Πριν από την ανάπτυξη συστήματος ΤΝ υψηλού κινδύνου που αναφέρεται στο άρθρο 6 παράγραφος 2, με την εξαίρεση συστημάτων ΤΝ υψηλού κινδύνου που προορίζονται για χρήση στον τομέα που αναφέρεται στο παράρτημα ΙΙΙ σημείο 2, οι φορείς εφαρμογής που είναι οργανισμοί δημόσιου δικαίου ή ιδιωτικές οντότητες που παρέχουν δημόσιες υπηρεσίες και οι φορείς εφαρμογής συστημάτων ΤΝ υψηλού κινδύνου που αναφέρονται στο παράρτημα ΙΙΙ σημείο 5 στοιχεία β) και γ) διενεργούν εκτίμηση των επιπτώσεων που μπορεί να έχει στα θεμελιώδη δικαιώματα η χρήση του συστήματος. Για τον σκοπό αυτόν, οι φορείς εφαρμογής διενεργούν εκτίμηση που περιλαμβάνει:
  - α) περιγραφή των διαδικασιών του φορέα εφαρμογής στις οποίες το σύστημα ΤΝ υψηλού κινδύνου θα χρησιμοποιείται σύμφωνα με τον επιδιωκόμενο σκοπό του·
  - β) περιγραφή του χρονικού διαστήματος εντός του οποίου και της συχνότητας με την οποία προορίζεται να χρησιμοποιηθεί κάθε σύστημα ΤΝ υψηλού κινδύνου·
  - γ) τις κατηγορίες φυσικών προσώπων και ομάδων που είναι πιθανό να επηρεαστούν από τη χρήση του στο συγκεκριμένο πλαίσιο·
  - δ) τους συγκεκριμένους κινδύνους βλάβης που είναι πιθανό να επηρεάσουν τις κατηγορίες φυσικών προσώπων ή ομάδων προσώπων που προσδιορίζονται δυνάμει του στοιχείου γ) της παρούσας παραγράφου, λαμβανομένων υπόψη των πληροφοριών που δίνει ο πάροχος δυνάμει του άρθρου 13·
  - ε) περιγραφή της εφαρμογής των μέτρων ανθρώπινης εποπτείας, σύμφωνα με τις οδηγίες χρήσης·
  - στ) τα μέτρα που πρέπει να λαμβάνονται σε περίπτωση επέλευσης των εν λόγω κινδύνων, συμπεριλαμβανομένων των ρυθμίσεων για την εσωτερική διακυβέρνηση και τους μηχανισμούς υποβολής καταγγελιών.

# Τεχνητή Νοημοσύνη

**GDPR**



**DPIA**

**(Data Protection Impact Assessment)**

*Άρθρο 35*

## Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.
2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.
3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:
  - α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,
  - β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή
  - γ) συστηματικής παρακολούθησης δημοσίας προσβάσιμου χώρου σε μεγάλη κλίμακα.

**AI Act**



**FRIA**

**(Fundamental Rights Impact Assessment)**

*Άρθρο 27*

## Εκτίμηση επιπτώσεων των συστημάτων ΤΝ υψηλού κινδύνου στα θεμελιώδη δικαιώματα

1. Πριν από την ανάπτυξη συστήματος ΤΝ υψηλού κινδύνου που αναφέρεται στο άρθρο 6 παράγραφος 2, με την εξαίρεση συστημάτων ΤΝ υψηλού κινδύνου που προορίζονται για χρήση στον τομέα που αναφέρεται στο παράρτημα ΙΙΙ σημείο 2, οι φορείς εφαρμογής που είναι οργανισμοί δημόσιου δικαίου ή ιδιωτικές οντότητες που παρέχουν δημόσιες υπηρεσίες και οι φορείς εφαρμογής συστημάτων ΤΝ υψηλού κινδύνου που αναφέρονται στο παράρτημα ΙΙΙ σημείο 5 στοιχεία β) και γ) διενεργούν εκτίμηση των επιπτώσεων που μπορεί να έχει στα θεμελιώδη δικαιώματα η χρήση του συστήματος. Για τον σκοπό αυτόν, οι φορείς εφαρμογής διενεργούν εκτίμηση που περιλαμβάνει:
  - α) περιγραφή των διαδικασιών του φορέα εφαρμογής στις οποίες το σύστημα ΤΝ υψηλού κινδύνου θα χρησιμοποιείται σύμφωνα με τον επιδιωκόμενο σκοπό του·
  - β) περιγραφή του χρονικού διαστήματος εντός του οποίου και της συχνότητας με την οποία προορίζεται να χρησιμοποιηθεί κάθε σύστημα ΤΝ υψηλού κινδύνου·
  - γ) τις κατηγορίες φυσικών προσώπων και ομάδων που είναι πιθανό να επηρεαστούν από τη χρήση του στο συγκεκριμένο πλαίσιο·
  - δ) τους συγκεκριμένους κινδύνους βλάβης που είναι πιθανό να επηρεάσουν τις κατηγορίες φυσικών προσώπων ή ομάδων προσώπων που προσδιορίζονται δυνάμει του στοιχείου γ) της παρούσας παραγράφου, λαμβανομένων υπόψη των πληροφοριών που δίνει ο πάροχος δυνάμει του άρθρου 13·
  - ε) περιγραφή της εφαρμογής των μέτρων ανθρώπινης εποπτείας, σύμφωνα με τις οδηγίες χρήσης·
  - στ) τα μέτρα που πρέπει να λαμβάνονται σε περίπτωση επέλευσης των εν λόγω κινδύνων, συμπεριλαμβανομένων των ρυθμίσεων για την εσωτερική διακυβέρνηση και τους μηχανισμούς υποβολής καταγγελιών.


# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

→ ↻ 🔍 edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template\_en

An official website of the European Union How do you know? ▾

European Data Protection Board

 ABOUT EDPB ▾ OUR WORK & TOOLS

European Data Protection Board



Home > Our Work & Tools > Public Consultations on our guidance > EDPB DPIA Template

## EDPB DPIA Template

Start Date: 14 April 2026

Public consultation reference: **DPIA Template**

End Date: 09 June 2026

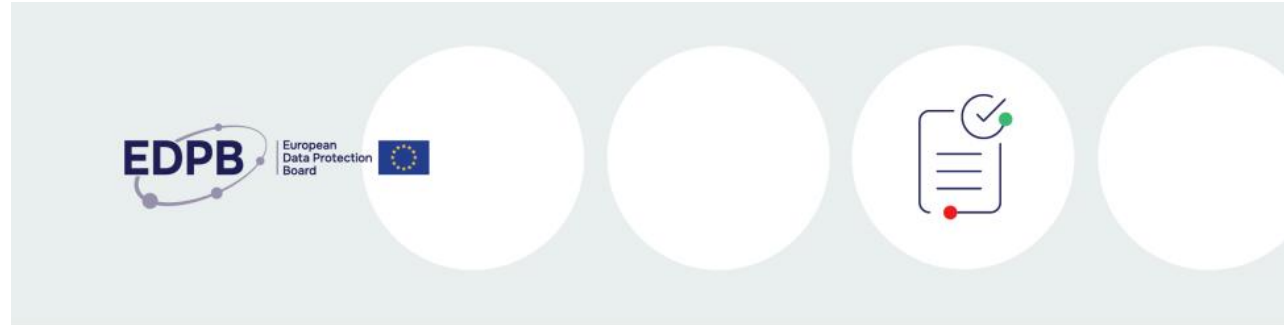
● Public consultation ongoing

The EDPB DPIA template is subject to a public consultation. After the public consultation is finished, the template will be finalised (subject to any appropriate modifications), after which all data protection authorities will begin the necessary steps to adopt this template as their unique template or as a 'meta-template' with which national specific templates will be compatible. In the meantime, organisations are encouraged to use this template and to provide feedback in the context of the public consultation.

[https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template\\_en](https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en)

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**



## Template [2026] for Data Protection Impact Assessment ('DPIA')

**Explainer**

Version 1.0

Adopted on 10 March 2026

[https://www.edpb.europa.eu/system/files/2026-04/edpb\\_dpia\\_template\\_explainer\\_2026\\_v1\\_en.pdf](https://www.edpb.europa.eu/system/files/2026-04/edpb_dpia_template_explainer_2026_v1_en.pdf)

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

## Table of Contents

<b>0</b>	<b>OVERVIEW OF THE PROCESSING .....</b>	<b>5</b>
	0.1 Controller(s).....	5
	0.2 Processor(s) and sub-processor(s) .....	5
	0.3 Name of the processing.....	5
	0.4 Planning of the processing .....	5
	0.5 DPIA technical sheet .....	5
<b>1</b>	<b>SYSTEMATIC DESCRIPTION OF THE PROCESSING .....</b>	<b>6</b>
	1.1 High-level description of the processing.....	6
	1.1.1 Processed personal data .....	6
	1.1.2 Purposes of the processing .....	6
	1.1.3 Secondary or compatible uses.....	6
	1.1.4 Nature, scope and context of the processing.....	6
	1.2 Functional description.....	7
	1.3 Means of processing, supporting assets and underlying architecture .....	7
	1.4 Compliance with approved codes of conduct .....	8

[https://www.edpb.europa.eu/system/files/2026-04/edpb\\_dpia\\_template\\_explainer\\_2026\\_v1\\_en.pdf](https://www.edpb.europa.eu/system/files/2026-04/edpb_dpia_template_explainer_2026_v1_en.pdf)

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

<b>2 ANALYSIS OF THE PROCESSING</b> .....	<b>8</b>
2.1 Lawfulness of the processing .....	8
2.1.1 Legal basis .....	8
2.1.2 Reasons to lift the processing prohibition .....	8
2.2 Data minimisation, retention periods, and data quality .....	8
2.2.1 Data minimisation and retention periods.....	8
2.2.2 Data quality .....	8
2.3 Measures supporting compliance .....	9
2.3.1 Measures supporting compliance with principles in Article 5(1)(a-f) GDPR .....	9
2.3.2 Measures supporting the exercise of data subjects' rights .....	9
2.3.3 Measures supporting compliance with other GDPR requirements .....	9
2.3.4 Measures supporting data protection by design and by default.....	9
2.3.5 Measures supporting security of the processing.....	9
<b>3 CONSIDERATIONS ON NECESSITY AND PROPORTIONALITY</b> .....	<b>10</b>
3.1 Impacts of the processing on the rights and freedoms of the data subjects.....	10
3.2 Assess the necessity of the processing.....	10
3.3 Assess the proportionality of the processing .....	10
<b>4 RISK ASSESSMENT AND MANAGEMENT</b> .....	<b>11</b>

[https://www.edpb.europa.eu/system/files/2026-04/edpb\\_dpia\\_template\\_explainer\\_2026\\_v1\\_en.pdf](https://www.edpb.europa.eu/system/files/2026-04/edpb_dpia_template_explainer_2026_v1_en.pdf)

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

<b>2 ANALYSIS OF THE PROCESSING</b> .....	8
2.1 <u>Lawfulness of the processing</u> .....	8
2.1.1 Legal basis .....	8
2.1.2 Reasons to lift the processing prohibition .....	8
2.2 Data minimisation, retention periods, and data quality .....	8
2.2.1 Data minimisation and retention periods.....	8
2.2.2 Data quality .....	8
2.3 Measures supporting compliance .....	9
2.3.1 Measures supporting compliance with principles in Article 5(1)(a-f) GDPR .....	9
2.3.2 Measures supporting the exercise of data subjects' rights .....	9
2.3.3 Measures supporting compliance with other GDPR requirements .....	9
2.3.4 Measures supporting data protection by design and by default.....	9
2.3.5 Measures supporting security of the processing.....	9
<b>3 CONSIDERATIONS ON <u>NECESSITY AND PROPORTIONALITY</u></b> .....	10
3.1 Impacts of the processing on the rights and freedoms of the data subjects.....	10
3.2 Assess the necessity of the processing.....	10
3.3 Assess the proportionality of the processing .....	10
<b>4 RISK ASSESSMENT AND MANAGEMENT</b> .....	11

**LLN**

**LLN**

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

**4 RISK ASSESSMENT AND MANAGEMENT.....11**

2 | Adopted

European Data Protection Board

---

4.1 Risk assessment and management .....	11
4.1.1 Impacts on the rights and freedoms of the data subjects caused by non-default, accidental, unlawful, or abnormal events.....	11
4.1.2 Method .....	11
4.1.3 Inherent risk assessment.....	11
4.2 Action plan .....	12
4.2.1 Additional mitigating measures .....	12
4.2.2 Residual risk assessment .....	12
4.2.3 Plan.....	13
<b>5 INVOLVEMENT OF INTERESTED PARTIES.....</b>	<b>13</b>
5.1 DPO advice .....	13
5.2 Views of data subjects or their representatives .....	13
<b>6 CONCLUSION AND DECISION.....</b>	<b>13</b>
<b>Annex 1 : SAS' GUIDELINES TO CONDUCT DPIAS .....</b>	<b>14</b>

[https://www.edpb.europa.eu/system/files/2026-04/edpb\\_dpia\\_template\\_explainer\\_2026\\_v1\\_en.pdf](https://www.edpb.europa.eu/system/files/2026-04/edpb_dpia_template_explainer_2026_v1_en.pdf)

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

<b>2 ANALYSIS OF THE PROCESSING</b> .....	8
2.1 <u>Lawfulness of the processing</u> .....	8
2.1.1 Legal basis .....	8
2.1.2 Reasons to lift the processing prohibition .....	8
2.2 Data minimisation, retention periods, and data quality .....	8
2.2.1 Data minimisation and retention periods.....	8
2.2.2 Data quality .....	8
2.3 Measures supporting compliance .....	9
2.3.1 Measures supporting compliance with principles in Article 5(1)(a-f) GDPR .....	9
2.3.2 Measures supporting the exercise of data subjects' rights .....	9
2.3.3 Measures supporting compliance with other GDPR requirements .....	9
2.3.4 Measures supporting data protection by design and by default.....	9
2.3.5 Measures supporting security of the processing.....	9
<b>3 CONSIDERATIONS ON <u>NECESSITY AND PROPORTIONALITY</u></b> .....	10
3.1 Impacts of the processing on the rights and freedoms of the data subjects.....	10
3.2 Assess the necessity of the processing.....	10
3.3 Assess the proportionality of the processing .....	10
<b>4 RISK ASSESSMENT AND MANAGEMENT</b> .....	11

**LLN**

**LLN**

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

**LLN**

<b>2 ANALYSIS OF THE PROCESSING</b> .....	8
2.1 <u>Lawfulness of the processing</u> .....	8
2.1.1 Legal basis.....	8
2.1.2 Reasons to lift the processing prohibition .....	8

## 2.1 Lawfulness of the processing

### 2.1.1 Legal basis

- 22 Analyse the legal basis of the processing. The analysis of each legal basis should be carried out in relation to each of the purposes of the processing (1.1.2) including secondary or compatible purposes (1.1.3).
- 23 If applicable, refer to an existing analysis (documented elsewhere, not in this template) or analyse the legitimate interests pursued by the controller or by a third party and conduct a balancing test<sup>4</sup>. If this analysis relies on any hypothesis on the implemented measures, residual risks, etc. please ensure they are properly reported in the appropriate sections in this template.

### 2.1.2 Reasons to lift the processing prohibition

- 24 If special categories of data are processed (see 1.1.1Processed personal data), the reasons that led to the lifting of the prohibition on processing special categories of data must be properly identified and justified.

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

**LLN**

<b>2 ANALYSIS OF THE PROCESSING</b> .....	8
2.1 <u>Lawfulness of the processing</u> .....	8
2.1.1 Legal basis.....	8
2.1.2 Reasons to lift the processing prohibition .....	8

## 2.1 Lawfulness of the processing

### 2.1.1 Legal basis

- 22 Analyse the legal basis of the processing. The analysis of each legal basis should be carried out in relation to each of the purposes of the processing (1.1.2) including secondary or compatible purposes (1.1.3).
- 23 If applicable, refer to an existing analysis (documented elsewhere, not in this template) or analyse the legitimate interests pursued by the controller or by a third party and conduct a balancing test<sup>4</sup>. If this analysis relies on any hypothesis on the implemented measures, residual risks, etc. please ensure they are properly reported in the appropriate sections in this template.

### 2.1.2 Reasons to lift the processing prohibition

- 24 If special categories of data are processed (see 1.1.1Processed personal data), the reasons that led to the lifting of the prohibition on processing special categories of data must be properly identified and justified.

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

**LLN**

<b>2 ANALYSIS OF THE PROCESSING</b> .....	8
2.1 <u>Lawfulness of the processing</u> .....	8
2.1.1 Legal basis.....	8
2.1.2 Reasons to lift the processing prohibition .....	8

## 2.1 Lawfulness of the processing

### 2.1.1 Legal basis

- 22 Analyse the legal basis of the processing. The analysis of each legal basis should be carried out in relation to each of the purposes of the processing (1.1.2) including secondary or compatible purposes (1.1.3).
- 23 If applicable, refer to an existing analysis (documented elsewhere, not in this template) or analyse the legitimate interests pursued by the controller or by a third party and conduct a balancing test<sup>4</sup>. If this analysis relies on any hypothesis on the implemented measures, residual risks, etc. please ensure they are properly reported in the appropriate sections in this template.

### 2.1.2 Reasons to lift the processing prohibition

- 24 If special categories of data are processed (see 1.1.1 Processed personal data), the reasons that led to the lifting of the prohibition on processing special categories of data must be properly identified and justified.

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

<b>2 ANALYSIS OF THE PROCESSING</b> .....	8
2.1 <u>Lawfulness of the processing</u> .....	8
2.1.1 Legal basis .....	8
2.1.2 Reasons to lift the processing prohibition .....	8
2.2 Data minimisation, retention periods, and data quality .....	8
2.2.1 Data minimisation and retention periods.....	8
2.2.2 Data quality .....	8
2.3 Measures supporting compliance .....	9
2.3.1 Measures supporting compliance with principles in Article 5(1)(a-f) GDPR .....	9
2.3.2 Measures supporting the exercise of data subjects' rights .....	9
2.3.3 Measures supporting compliance with other GDPR requirements .....	9
2.3.4 Measures supporting data protection by design and by default.....	9
2.3.5 Measures supporting security of the processing.....	9
<b>3 CONSIDERATIONS ON <u>NECESSITY AND PROPORTIONALITY</u></b> .....	10
3.1 Impacts of the processing on the rights and freedoms of the data subjects.....	10
3.2 Assess the necessity of the processing.....	10
3.3 Assess the proportionality of the processing .....	10
<b>4 RISK ASSESSMENT AND MANAGEMENT</b> .....	11

**LLN**

**LLN**

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

**LLN**

<b>3 CONSIDERATIONS ON NECESSITY AND PROPORTIONALITY</b> .....	10
3.1 Impacts of the processing on the rights and freedoms of the data subjects.....	10
3.2 Assess the necessity of the processing.....	10
3.3 Assess the proportionality of the processing .....	10

## 3.1 Impacts of the processing on the rights and freedoms of the data subjects

32 Explain how the threats that the planned processing (as it has been designed and is projected to be implemented, including technical, legal/contractual and organisational measures to mitigate risk) poses to the rights and freedoms of the data subjects can be materialised and identify their impacts and all possible risk sources. These are risks that exist even if everything works exactly as designed and all actors follow the rules.

These threats flow, mainly, from the processed personal data (1.1.1), the very purpose of the processing (1.1.2) and its nature, scope and context (1.1.4). Even if the processing is correctly implemented and works as specified, there are risks tied to its inherent and structural characteristics: everything goes as intended, but design choices themselves create risks for data subjects' rights and freedoms, even where there is no failure or attack. A threat is any circumstance or event with the potential to adversely impact data subject's rights and freedoms (for example, linking, identifying, inaccuracy or data disclosure) and it may cause physical, material or non-material damage to data subjects.

A risk source is the origin or underlying cause from which a threat can materialise. Typical examples are the characteristics of the processing itself i.e., its purpose, wrong design and weaknesses (for example, use of unique identifiers, or long retention periods), exposures, etc.

Impact is the consequences that can be expected from the threat materialisation, always considering data subject's rights and freedoms (see recital 75 GDPR, for example).

## 3.2 Assess the necessity of the processing

33 Assess the necessity of the processing<sup>6</sup>. Evaluate if the envisaged processing is effective and the least intrusive for the data subject's rights and freedoms. Analyse if the processing demonstrably works as intended, at least to the appropriate or required level. Provide evidence (for example, concerning the different considered alternatives and their effectiveness in achieving the purpose) and justification.

# Τεχνητή Νοημοσύνη

**GDPR: DPIA**

**LLN**

<b>3 CONSIDERATIONS ON NECESSITY AND PROPORTIONALITY</b> .....	10
3.1 Impacts of the processing on the rights and freedoms of the data subjects.....	10
3.2 Assess the necessity of the processing.....	10
3.3 Assess the proportionality of the processing .....	10

## 3.1 Impacts of the processing on the rights and freedoms of the data subjects

32 Explain how the threats that the planned processing (as it has been designed and is projected to be implemented, including technical, legal/contractual and organisational measures to mitigate risk) poses to the rights and freedoms of the data subjects can be materialised and identify their impacts and all possible risk sources. These are risks that exist even if everything works exactly as designed and all actors follow the rules.

These threats flow, mainly, from the processed personal data (1.1.1), the very purpose of the processing (1.1.2) and its nature, scope and context (1.1.4). Even if the processing is correctly implemented and works as specified, there are risks tied to its inherent and structural characteristics: everything goes as intended, but design choices themselves create risks for data subjects' rights and freedoms, even where there is no failure or attack. A threat is any circumstance or event with the potential to adversely impact data subject's rights and freedoms (for example, linking, identifying, inaccuracy or data disclosure) and it may cause physical, material or non-material damage to data subjects.

A risk source is the origin or underlying cause from which a threat can materialise. Typical examples are the characteristics of the processing itself i.e., its purpose, wrong design and weaknesses (for example, use of unique identifiers, or long retention periods), exposures, etc.

Impact is the consequences that can be expected from the threat materialisation, always considering data subject's rights and freedoms (see recital 75 GDPR, for example).

## 3.2 Assess the necessity of the processing

33 Assess the necessity of the processing<sup>6</sup>. Evaluate if the envisaged processing is effective and the least intrusive for the data subject's rights and freedoms. Analyse if the processing demonstrably works as intended, at least to the appropriate or required level. Provide evidence (for example, concerning the different considered alternatives and their effectiveness in achieving the purpose) and justification.

and could not make claims against any jurisdiction other than Portugal, and although the case against Switzerland only partially succeeded (the association was found to have a case, but not the individuals), the general feeling is that these cases have paved the way for more climate change cases in the future based on the European Convention of Human Rights (ECHR).

The Council of Europe is considering a further instrument to make the right to a healthy environment an incontestable part of the ECHR, and has produced a **document** with background and arguments.

The 2024 case with the most human interest was ***Dian v. Denmark*** (44002/22), concerning a Romanian national of 61, who was found guilty of begging on a pedestrian street in Copenhagen and also of insulting a police inspector in the exercise of her functions. He was sentenced to 20 days' imprisonment, since he had a previous conviction for begging. He called in aid a previous ECtHR decision which found that a sentence for begging could be a breach of Article 8 (respect for private life). But the court said that there was no absolute right to beg, and that each case depended on its circumstances. In this case, he had other sources of income, roughly €135 in his pocket, and a house back in Romania. His case failed.

<https://www.lawgazette.co.uk/commentary-and-opinion/what-did-the-european-court-of-human-rights-do-in-2024/5122006.article>

and could not make claims against any jurisdiction other than Portugal, and although the case against Switzerland only partially succeeded (the association was found to have a case, but not the individuals), the general feeling is that these cases have paved the way for more climate change cases in the future based on the European Convention of Human Rights (ECHR).

The Council of Europe is considering a further instrument to make the right to a healthy environment an incontestable part of the ECHR, and has produced a **document** with background and arguments.

The 2024 case with the most human interest was ***Dian v. Denmark*** (44002/22), concerning a Romanian national of 61, who was found guilty of begging on a pedestrian street in Copenhagen and also of insulting a police inspector in the exercise of her functions. He was sentenced to 20 days' imprisonment, since he had a previous conviction for begging. He called in aid a previous ECtHR decision which found that a sentence for begging could be a breach of Article 8 (respect for private life). But the court said that there was no absolute right to beg, and that each case depended on its circumstances. In this case, he had other sources of income, roughly €135 in his pocket, and a house back in Romania. His case failed.

<https://www.lawgazette.co.uk/commentary-and-opinion/what-did-the-european-court-of-human-rights-do-in-2024/5122006.article>



lawgazette.co.uk/commentary-and-opinion/what-did-the-european-court-of-human-rights-do-in-2024/5122006.article



NEWS ▾

ANALYSIS ▾

LAW ▾

PRACTICE ▾

IN-HOUSE ▾

PEOPLE ▾

JOBS ▾

DIRE

and could not make claims against any jurisdiction other than Portugal, and although the case against Switzerland only partially succeeded (the association was found to have a case, but not the individuals), the general feeling is that these cases have paved the way for more climate change cases in the future based on the European Convention of Human Rights (ECHR).

The Council of Europe is considering a further instrument to make the right to a healthy environment an incontestable part of the ECHR, and has produced a **document** with background and arguments.

The 2024 case with the most human interest was ***Dian v. Denmark*** (44002/22), concerning a Romanian national of 61, who was found guilty of begging on a pedestrian street in Copenhagen and also of insulting a police inspector in the exercise of her functions. He was sentenced to 20 days' imprisonment, since he had a previous conviction for begging. He called in aid a previous ECtHR decision which found that a sentence for begging could be a breach of Article 8 (respect for private life). But the court said that there was no absolute right to beg, and that each case depended on its circumstances. In this case, he had other sources of income, roughly €135 in his pocket, and a house back in Romania. His case failed.

<https://www.lawgazette.co.uk/commentary-and-opinion/what-did-the-european-court-of-human-rights-do-in-2024/5122006.article>



lawgazette.co.uk/commentary-and-opinion/what-did-the-european-court-of-human-rights-do-in-2024/5122006.article



NEWS ▾

ANALYSIS ▾

LAW ▾

PRACTICE ▾

IN-HOUSE ▾

PEOPLE ▾

JOBS ▾

DIRE

and could not make claims against any jurisdiction other than Portugal, and although the case against Switzerland only partially succeeded (the association was found to have a case, but not the individuals), the general feeling is that these cases have paved the way for more climate change cases in the future based on the European Convention of Human Rights (ECHR).

The Council of Europe is considering a further instrument to make the right to a healthy environment an incontestable part of the ECHR, and has produced a **document** with background and arguments.

The 2024 case with the most human interest was *Dian v. Denmark* (44002/22), concerning a Romanian national of 61, who was found guilty of begging on a pedestrian street in Copenhagen and also of insulting a police inspector in the exercise of her functions. He was sentenced to 20 days' imprisonment, since he had a previous conviction for begging. He called in aid a previous ECtHR decision which found that a sentence for begging could be a breach of Article 8 (respect for private life). But the court said that there was no absolute right to beg, and that each case depended on its circumstances. In this case, he had other sources of income, roughly €135 in his pocket, and a house back in Romania. His case failed.

<https://www.lawgazette.co.uk/commentary-and-opinion/what-did-the-european-court-of-human-rights-do-in-2024/5122006.article>

# JURISTnews

Law students reporting the rule of law in crisis

News ▾

Dispatches ▾

Commentary ▾

Features ▾

Topics

Rule of Law ▾



## UK to decriminalize rough sleeping

Lara Zand | BPP U. Law School, GB

JUNE 12, 2025 07:04:06 PM



<https://www.jurist.org/news/2025/06/uk-to-decriminalize-rough-sleeping/>

## UK to decriminalize rough sleeping

Lara Zand | BPP U. Law School, GB

JUNE 12, 2025 07:04:06 PM



The UK government announced on Monday that it plans to scrap a Georgian-era law that made “rough sleeping” a criminal offense.

The official **statement** promised to abolish the 200-year-old statute by spring of next year.

“We are drawing a line under nearly two centuries of injustice towards some of the most vulnerable in society,” Deputy Prime Minister and Housing Secretary Angela Rayner said. “No one should ever be criminalised simply for sleeping rough and by scrapping this cruel and outdated law, we are making sure that can never happen again.”

The Vagrancy Act was introduced in 1824 in response to rising homelessness rates in the aftermath of the Napoleonic Wars and Industrial Revolution. Under the act, convictions for rough sleeping—sleeping in the street—or begging can attract fines of up to £1,000 and occasionally imprisonment.

The UK Parliament voted to repeal the act in April 2022, but enacting the repeal was delayed until the government brought in replacement legislation and the law continued in force. Single Homeless Project, a UK charity, **reported** that between April 2022 and June 2024, 177 people were arrested under the law.

The Minister for Homelessness Rushanara Ali agreed that the act was “neither just nor fit for purpose” and said government efforts going forwards would focus on the root causes of homelessness.

The government has pledged to introduce new offenses of facilitating begging for gain and trespassing with the intention of committing a crime, which aim to crack down on organized begging facilitated by criminal gangs. It also committed to increasing funding for homelessness services by an additional £233 million this financial year.

<https://www.jurist.org/news/2025/06/uk-to-decriminalize-rough-sleeping/>

-Advertisement-  
Ad by CRITEO

Report this ad

Ad choices ▶

TECH

# Update: Head of Romania's telecommunications regulatory authority calls for immediate suspension of TikTok amid electoral scandal

-Advertisement-

<https://www.romania-insider.com/head-ancom-calls-immediate-suspension-tiktok-romania-elections-2024>

TRAVEL GUIDES > INTERNATIONAL > TRAVEL ETIQUETTE

# The Beloved Romantic Tradition That Is Banned In Two Of Italy's Most Popular Cities

By [Anna Robinson](#) · Feb. 10, 2025 1:00 pm EST




<https://www.explore.com/1779874/love-locks-popular-tradition-banned-two-italy-popular-cities-rome-venice/>



<https://www.explore.com/1779874/love-locks-popular-tradition-banned-two-italy-popular-cities-rome-venice/>

# Facial recognition in school renders Sweden's first GDPR fine

 Published: 21 August 2019

The Swedish DPA has fined a municipality 200 000 SEK (approximately 20 000 euros) for using facial recognition technology to monitor the attendance of students in school

A school in northern Sweden has conducted a pilot using facial recognition to keep track of students' attendance in school. The test run was conducted in one school class for a limited period of time.

<https://www.imy.se/en/about-us/arkiv/nyhetsarkiv/facial-recognition-in-school-renders-swedens-first-gdpr-fine>

itv.com/news/london/2026-04-11/almost-100-people-arrested-at-protest-against-palestine-action-ban-in-london

LIVE FILM CATEGORIES NEWS MY LIST

More ▾

## More than 500 arrested at protest against Palestine Action ban in London

LONDON | METROPOLITAN POLICE | Sunday 12 April 2026 at 11:59am



<https://www.itv.com/news/london/2026-04-11/almost-100-people-arrested-at-protest-against-palestine-action-ban-in-london>

ADVERTISEMENT

**Flashcloud**

Web Hosting  
Done Better

Learn more



Better Hosting, In a Flash!

Free website, free domain for life, and real support when you need it.

Flashcloud

Open >

INNOVATION > SCIENCE

# FBI Pulled Deleted Signal Messages From An iPhone Without Breaking Encryption

By **Lars Daniel**, Contributor. © Lars Daniel covers digital evidence and forensic...

Follow Author

Published Apr 10, 2026, 09:00am EDT



NOW PLAYING: KEN CHENAULT SHARES WHAT A GOOD LEAD



<https://www.forbes.com/sites/larsdaniel/2026/04/10/fbi-pulled-deleted-signal-messages-from-an-iphone-without-breaking-encryption/>

# Social media age verification laws by country

2 languages

its hide

Article Talk

Read Edit View history Tools

Appearance hide

From Wikipedia, the free encyclopedia



This article **may require copy editing** for grammar, style, cohesion, tone, or spelling. You can assist by [editing it](#). (February 2026) *(Learn how and when to remove this message)*

.merica  
merica  
a  
o  
nces

Multiple countries have passed laws to require [age verification](#) for [social media](#) services as an attempt to address certain harms on social media. The passage of such laws began primarily after Australia's social media ban for under-16-year-olds was passed in November 2024, and came into force on 10 December 2025. The ban began in the United States at the state level after Utah passed the [Utah Social Media Regulation Act](#) in March 2023.<sup>[1][2][3][4]</sup> These bills and laws vary a lot with some of them restricting access only to certain features or distinguish between different users online and which could lead to companies requiring age verification to have such restrictions such as the [Kids Online Safety Act](#) or require it outright and ban users under a certain age such as the [Online Safety Amendment](#) in Australia which bans anyone under 16 from holding a social media account including [YouTube](#).<sup>[5][6]</sup>

Text

- Small
- Standard
- Large

Width

- Standard
- Wide

Color (beta)

- Automatic

[https://en.wikipedia.org/wiki/Social\\_media\\_age\\_verification\\_laws\\_by\\_country](https://en.wikipedia.org/wiki/Social_media_age_verification_laws_by_country)



# European age verification app to keep children safe online

## NEWS ARTICLE

15 April 2026 — Directorate-General for Communication — 1 min read



[https://commission.europa.eu/news-and-media/news/european-age-verification-app-keep-children-safe-online-2026-04-15\\_en](https://commission.europa.eu/news-and-media/news/european-age-verification-app-keep-children-safe-online-2026-04-15_en)

# Ευχαριστώ!!!

Γιώργος Μπουχάγιαρ  
Vrije Universiteit Brussel & Ιόνιο Πανεπιστήμιο

Email:

[georgios.bouchagiar@vub.be](mailto:georgios.bouchagiar@vub.be)

[georgebouchayar@ionio.gr](mailto:georgebouchayar@ionio.gr)