



Ευρωπαϊκή
Επιτροπή

Η πράξη για τις ψηφιακές υπηρεσίες (DSA) με απλά λόγια

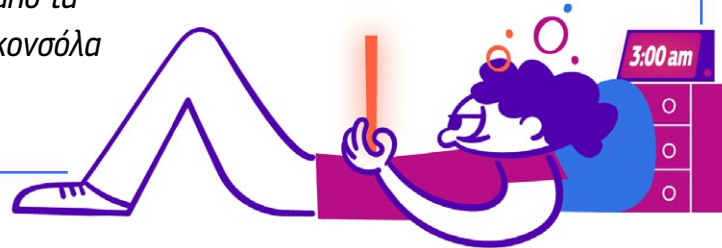
Τι πρέπει να κάνουν οι
επιγραμμικές (online)
πλατφόρμες για την προστασία
παιδιών και εφήβων
στο διαδίκτυο



Τι είναι η πράξη για τις ψηφιακές υπηρεσίες (DSA);

Οι επιγραμμικές (online) πλατφόρμες είναι σημαντικό κομμάτι της καθημερινότητας των παιδιών και των εφήβων, καθώς σε αυτές επικοινωνούν με τους φίλους τους, παρακολουθούν βίντεο, παίζουν ή μαθαίνουν καινούργια πράγματα. Όμως το διαδίκτυο επιφυλάσσει σοβαρούς κινδύνους. Τα παιδιά και οι έφηβοι μπορεί:

- ▶ να υποστούν κυβερνοεκφοβισμό (cyberbullying);
- ▶ να τους προσεγγίσουν άγνωστοι με κακές προθέσεις;
- ▶ να δουν επιβλαβές ή ανησυχητικό περιεχόμενο με το οποίο θα αισθανθούν άβολα ή θα νιώσουν φόβο ή αναστάτωση;
- ▶ να πιεστούν να πραγματοποιήσουν αγορές;
- ▶ να συμμετάσχουν σε επικίνδυνες προκλήσεις;
- ▶ να μην μπορούν να αφήσουν το κινητό από τα χέρια τους ή να απενεργοποιήσουν την κονσόλα παιχνιδιού.



Για να βοηθήσει να γίνει ασφαλέστερο το διαδίκτυο, το 2022 η Ευρωπαϊκή Ένωση (ΕΕ) δημιούργησε την πράξη για τις ψηφιακές υπηρεσίες (DSA), η οποία ισχύει για τις επιγραμμικές πλατφόρμες (ευρωπαϊκές και μη) που είναι διαθέσιμες στην ΕΕ. Στόχος της είναι να προστατεύσει από τους παραπάνω αλλά και από άλλους κινδύνους όλους τους χρήστες του διαδικτύου —μεταξύ αυτών παιδιά και εφήβους—, καθώς και να προστατεύσει τα θεμελιώδη δικαιώματά τους στο διαδίκτυο.

Όλες οι επιγραμμικές πλατφόρμες οφείλουν να τηρούν όσα προβλέπονται στην πράξη αυτή και να προάγουν τη διαδικτυακή ασφάλεια των χρηστών στην ΕΕ.

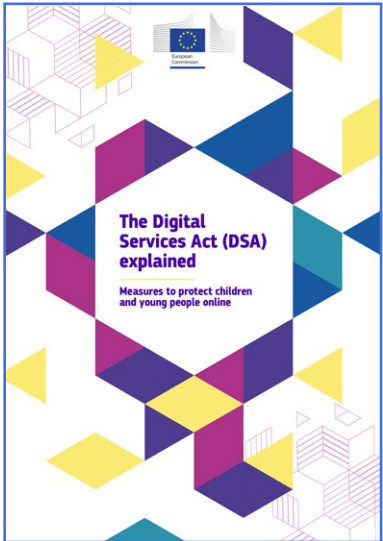


Πώς προστατεύει η DSA τα παιδιά και τους εφήβους;

Σύμφωνα με την DSA, **οι επιγραμμικές πλατφόρμες πρέπει να προσφέρουν στους ανηλίκους που χρησιμοποιούν τις υπηρεσίες τους υψηλό επίπεδο ιδιωτικότητας, ασφάλειας και προστασίας.**

Αυτό σημαίνει ότι τα παιδιά και οι έφηβοι θα πρέπει να αισθάνονται προστατευμένοι και ασφαλείς όταν χρησιμοποιούν εφαρμογές, μέσα κοινωνικής δικτύωσης και παιχνίδια που υπάγονται σε αυτόν τον νόμο. Οι μεγαλύτερες πλατφόρμες, οι οποίες αριθμούν πάνω από 45 εκατομμύρια χρήστες στην ΕΕ, όπως το TikTok, το Instagram και το Snapchat, οφείλουν επίσης να εντοπίζουν και να αξιολογούν άλλους πιθανούς κινδύνους για τα παιδιά και τους εφήβους που χρησιμοποιούν τις υπηρεσίες τους.

Τον Ιούλιο του 2025 η Ευρωπαϊκή Επιτροπή δημοσίευσε κατευθυντήριες γραμμές για την προστασία των ανηλίκων ώστε να γίνει κατανοητό από όλες τις πλατφόρμες τι πρέπει να κάνουν για την προστασία παιδιών και εφήβων στο διαδίκτυο. Το παρόν εγχειρίδιο εξηγεί πώς λειτουργούν αυτές οι κατευθυντήριες γραμμές.



Θέλετε να μάθετε περισσότερα για την DSA; Δείτε αυτό το εγχειρίδιο που εξηγεί τα μέτρα για την προστασία των παιδιών και των νέων στο διαδίκτυο.

Περιεχόμενα

1. Ποιοι πρέπει να τηρούν τις κατευθυντήριες γραμμές για την προστασία των ανηλίκων;	4
2. Ποιες είναι οι βασικές αρχές;	5
3. Συστάσεις	6
α. Εκτίμηση κινδύνων: σε κάθε πλατφόρμα υπάρχουν διαφορετικοί κίνδυνοι	6
β. Διασφάλιση της ηλικίας: με ποιον τρόπο οι πλατφόρμες ελέγχουν την ηλικία σας	6
γ. Εγγραφή: πληροφόρηση και ενδυνάμωση από το πρώτο βήμα	10
δ. Ρυθμίσεις λογαριασμού: πώς να ελέγχετε την ιδιωτικότητα και την ασφάλειά σας	11
ε. Διεπαφές: σχεδιάζοντας εύχρηστες και ασφαλείς πλατφόρμες	13
στ. Συστήματα συστάσεων και λειτουργίες αναζήτησης: βοηθώντας τα παιδιά να διατηρούν τον έλεγχο	14
ζ. Εμπορικές πρακτικές: βοηθώντας τους νέους να κατανοήσουν τι προωθείται και πωλείται	15
η. Έλεγχος περιεχομένου: ασφάλεια και σεβασμός στις πλατφόρμες	16
θ. Υποβολή αναφορών: διευκολύνοντας τους ανηλίκους να μιλήσουν και να αναζητήσουν βοήθεια	17
ι. Εργαλεία για γονείς και κηδεμόνες	18
4. Ποιος εξασφαλίζει ότι τηρούνται οι κανόνες της DSA;	19
5. Τι θα συμβεί στη συνέχεια;	19
Πού μπορείτε να βρείτε περισσότερες πληροφορίες και βοήθεια;	24

Η παρούσα έκδοση είναι απλώς ενημερωτική και δεν αποτελεί νομικό έγγραφο.

1. Ποιοι πρέπει να τηρούν τις κατευθυντήριες γραμμές για την προστασία των ανηλίκων;

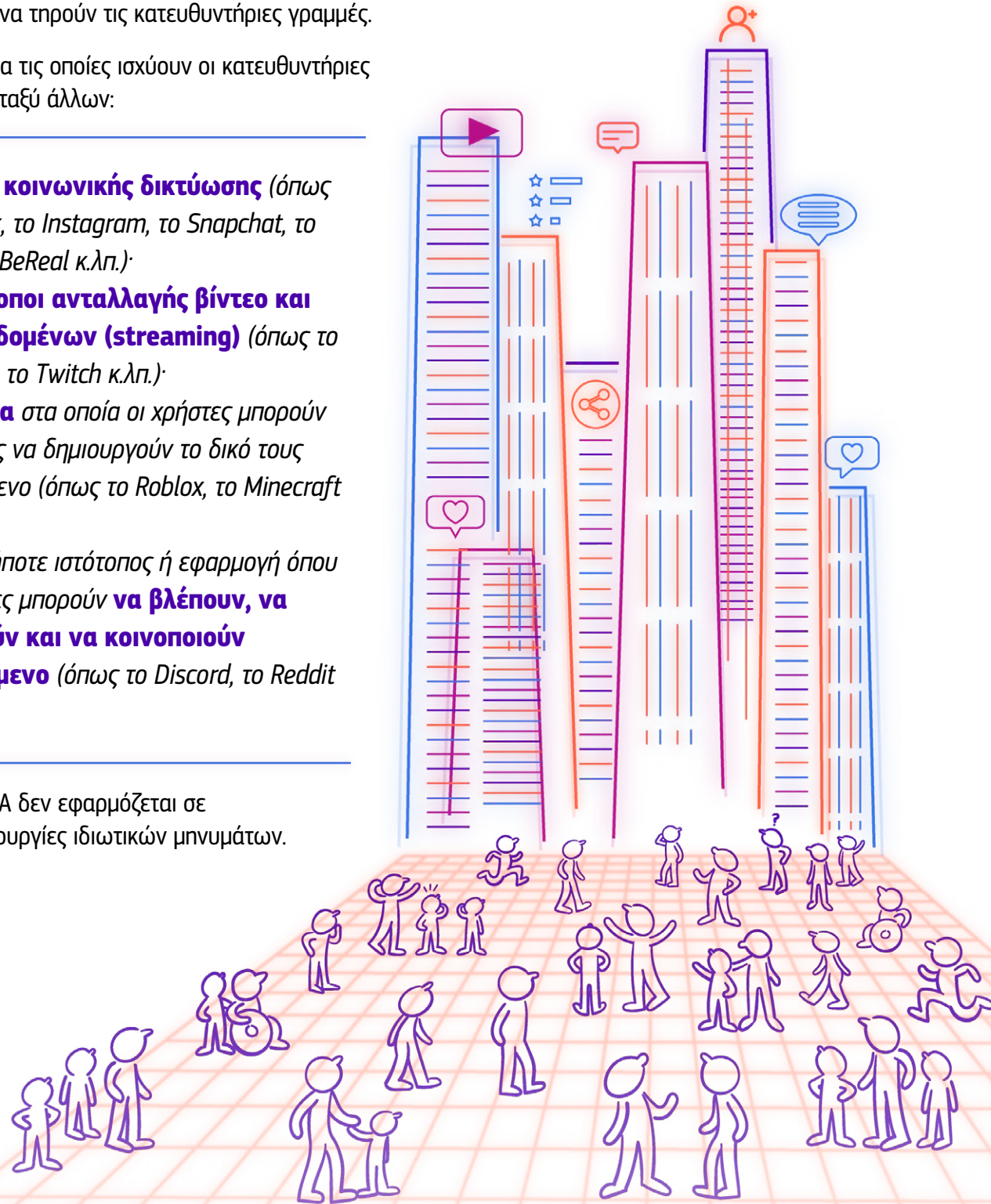
Εάν μια πλατφόρμα χρησιμοποιείται από παιδιά και εφήβους —ή εάν είναι πιθανό να έχουν πρόσβαση σε αυτή— τότε η πλατφόρμα αυτή **πρέπει** να τηρεί τους κανόνες και τις κατευθυντήριες γραμμές της DSA για την προστασία των ανηλίκων.

Ιστότοποι που έχουν σχεδιαστεί για ενήλικες δεν αρκεί να δηλώνουν απλώς ότι, σύμφωνα με τους κανόνες τους, «δεν επιτρέπεται η πρόσβαση σε παιδιά» και να αγνοούν την πραγματικότητα. Εάν γνωρίζουν ότι το περιεχόμενό τους είναι προσβάσιμο και σε νεότερα άτομα, οφείλουν να τηρούν τις κατευθυντήριες γραμμές.

Οι πλατφόρμες για τις οποίες ισχύουν οι κατευθυντήριες γραμμές είναι, μεταξύ άλλων:

- ▶ **τα μέσα κοινωνικής δικτύωσης** (όπως το TikTok, το Instagram, το Snapchat, το Yubo, το BeReal κ.λπ.)·
- ▶ **οι ιστότοποι ανταλλαγής βίντεο και ροής δεδομένων (streaming)** (όπως το YouTube, το Twitch κ.λπ.)·
- ▶ **παιχνίδια** στα οποία οι χρήστες μπορούν παίζοντας να δημιουργούν το δικό τους περιεχόμενο (όπως το Roblox, το Minecraft κ.λπ.)·
- ▶ **οποιοσδήποτε ιστότοπος ή εφαρμογή όπου οι χρήστες μπορούν να βλέπουν, να αναρτούν και να κοινοποιούν περιεχόμενο** (όπως το Discord, το Reddit κ.λπ.).

Σημείωση: Το DSA δεν εφαρμόζεται σε υπηρεσίες ή λειτουργίες ιδιωτικών μηνυμάτων.



2. Ποιες είναι οι βασικές αρχές;

Οι κατευθυντήριες γραμμές βασίζονται σε τρεις κεντρικές ιδέες:

1. Τα δικαιώματα των παιδιών έχουν προτεραιότητα

Οι πλατφόρμες πρέπει να σέβονται τα δικαιώματα των παιδιών και να λειτουργούν πάντοτε με γνώμονα το συμφέρον τους. Τα δικαιώματα αυτά περιλαμβάνουν:

- ▶ την προστασία·
- ▶ την απαγόρευση των διακρίσεων·
- ▶ την ένταξη·
- ▶ την ιδιωτικότητα·
- ▶ την πρόσβαση σε πληροφορίες και εκπαίδευση·
- ▶ την ελευθερία της έκφρασης·
- ▶ τη συμμετοχή.



Αυτό σημαίνει ότι οι υπηρεσίες τους θα πρέπει να σχεδιάζονται, να αναπτύσσονται και να λειτουργούν έτσι ώστε να διασφαλίζονται πάντοτε η ασφάλεια, η ιδιωτικότητα και η προστασία των παιδιών.

2. Ασφάλεια από τον σχεδιασμό

Οι πλατφόρμες δεν θα πρέπει να περιμένουν να προκύψουν προβλήματα. Αντίθετα, θα πρέπει να φροντίζουν ώστε να υπάρχει εξαρχής ιδιωτικότητα, ασφάλεια και προστασία στις υπηρεσίες τους. Τα επιμέρους χαρακτηριστικά θα πρέπει να είναι κατάλληλα για τις διάφορες ηλικίες και τα στάδια ανάπτυξης των παιδιών.

3. Κατανόηση των αναγκών των χρηστών

Οι πλατφόρμες πρέπει να εξετάζουν προσεκτικά πώς χρησιμοποιούν τα παιδιά και οι έφηβοι τις υπηρεσίες τους και ποιους κινδύνους ενδέχεται να αντιμετωπίσουν, όπως:

- ▶ κυβερνοεκφοβισμό·
- ▶ επιβλαβές περιεχόμενο·
- ▶ υπερβολική χρήση.



Έπειτα, πρέπει να βρίσκουν λύσεις για τη μείωση των κινδύνων αυτών.

3. Συστάσεις

Ας ρίξουμε μια ματιά στις συστάσεις που πρέπει να τηρούν οι πλατφόρμες για την προστασία παιδιών και εφήβων στο διαδίκτυο.

α. Εκτίμηση κινδύνων: σε κάθε πλατφόρμα υπάρχουν διαφορετικοί κίνδυνοι

Οι κατευθυντήριες γραμμές συνιστούν στις πλατφόρμες να **ελέγχουν τακτικά** κατά πόσο οι υπηρεσίες τους εμπεριέχουν **κινδύνους για παιδιά και εφήβους** και να κατανοούν το πώς και το γιατί συμβαίνει αυτό. Θα πρέπει να βρίσκουν τη σωστή ισορροπία ανάμεσα:

- ▶ στο να επιτρέπουν στα παιδιά και στους εφήβους να κοινοποιούν το περιεχόμενό τους, τις ιδέες και τις σκέψεις τους
 - ▶ στο να τους δίνουν την ευκαιρία να εξερευνήσουν, να παίξουν και να μάθουν καινούργια πράγματα στο διαδίκτυο...
- ...και στο να εγγυώνται ταυτόχρονα την ασφάλειά τους!

Μόλις εντοπιστούν κίνδυνοι, οι πλατφόρμες πρέπει να ανταποκρίνονται παρέχοντας αποτελεσματικές λύσεις —χωρίς να περιορίζουν τις σημαντικές ευκαιρίες και τα οφέλη που μπορούν να απολαμβάνουν τα παιδιά στο διαδίκτυο.

β. Διασφάλιση της ηλικίας: με ποιον τρόπο οι πλατφόρμες ελέγχουν την ηλικία σας

Για να γίνουν οι πλατφόρμες πιο ασφαλείς —και για να μη χρησιμοποιούν τα παιδιά και οι έφηβοι υπηρεσίες που δεν είναι κατάλληλες για την ηλικία τους— είναι σημαντικό να διασφαλίζεται ότι οι χρήστες είναι στην κατάλληλη ηλικία για να έχουν πρόσβαση σε συγκεκριμένο περιεχόμενο.

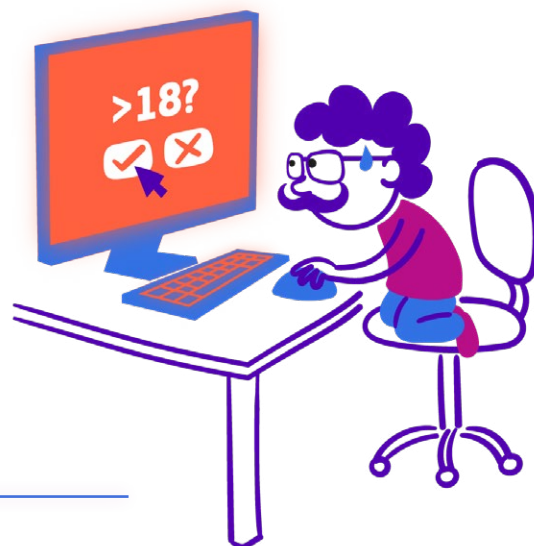
Σε αυτό χρησιμεύει η **διασφάλιση της ηλικίας**.

Η διασφάλιση της ηλικίας γίνεται με τη χρήση εργαλείων με τα οποία μπορεί:

- ▶ να εξακριβωθεί ή να εκτιμηθεί η ηλικία ενός χρήστη· ή
- ▶ να επιβεβαιωθεί εάν κάποιο άτομο είναι μεγαλύτερο ή μικρότερο από μια συγκεκριμένη ηλικία.

Το γνωρίζετε;

Πρέπει να είστε άνω των 13 ετών για να χρησιμοποιείτε το TikTok, το Snapchat, το Instagram, το BeReal και το Steam!



Τρόποι διασφάλισης ηλικίας

Υπάρχουν 3 κύριοι τρόποι με τους οποίους οι πλατφόρμες μπορούν να ελέγχουν την ηλικία ενός χρήστη:

1. Δήλωση του χρήστη

Εισάγετε την ημερομηνία γέννησής σας ή επιλέγετε «Ναι, είμαι άνω των 13 ετών» ή «Ναι, είμαι άνω των 18 ετών». Ο τρόπος αυτός είναι γρήγορος, αλλά μπορεί εύκολα να πει κανείς ψέματα, συνεπώς **δεν είναι ιδιαίτερα αποτελεσματικός ούτε αξιόπιστος**.

2. Εκτίμηση ηλικίας

Η τεχνολογία εκτιμά την ηλικία σας με βάση στοιχεία όπως:

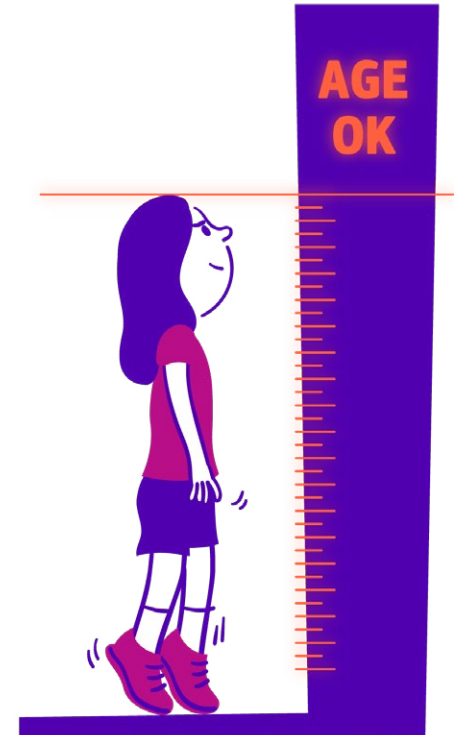
- > σάρωση προσώπου·
- > τρόπος πληκτρολόγησης·
- > τα ενδιαφέροντά σας.

Ο τρόπος αυτός δεν είναι τέλειος —δεν εντοπίζει την ακριβή ηλικία σας, ενώ ενδέχεται και να **παραβιάζει** την ιδιωτικότητά σας.

3. Επαλήθευση ηλικίας

Αυτή είναι η **πιο ακριβής** μέθοδος από όλες. Ελέγχει την ηλικία σας με βάση:

- > επίσημα έγγραφα, όπως το διαβατήριό σας·
- > αξιόπιστες ψηφιακές ταυτότητες, όπως ένα δελτίο ταυτότητας που εκδίδεται από το κράτος, ή το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ (EU Digital Identity Wallet). Η τελευταία μέθοδος **προστατεύει την ιδιωτικότητά σας**, καθώς επιτρέπει στους χρήστες να αποδείξουν την ηλικία τους χωρίς να αποκαλύψουν άλλα προσωπικά τους στοιχεία.



Τι είναι το πορτοφόλι ψηφιακής ταυτότητας της ΕΕ; Είναι μια δωρεάν εφαρμογή (διαθέσιμη από το 2026) που βοηθά τους κατοίκους της Ευρώπης:

- ▶ να διατηρούν σημαντικά έγγραφα τους ασφαλή σε ένα σημείο·
- ▶ να αποδεικνύουν την ταυτότητά τους τόσο στο διαδίκτυο όσο και διά ζώσης.

Μοιάζει με ψηφιακό πορτοφόλι όπου μπορείτε να μεταφέρετε την ταυτότητά σας και άλλα σημαντικά έγγραφα.



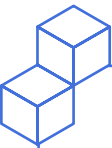
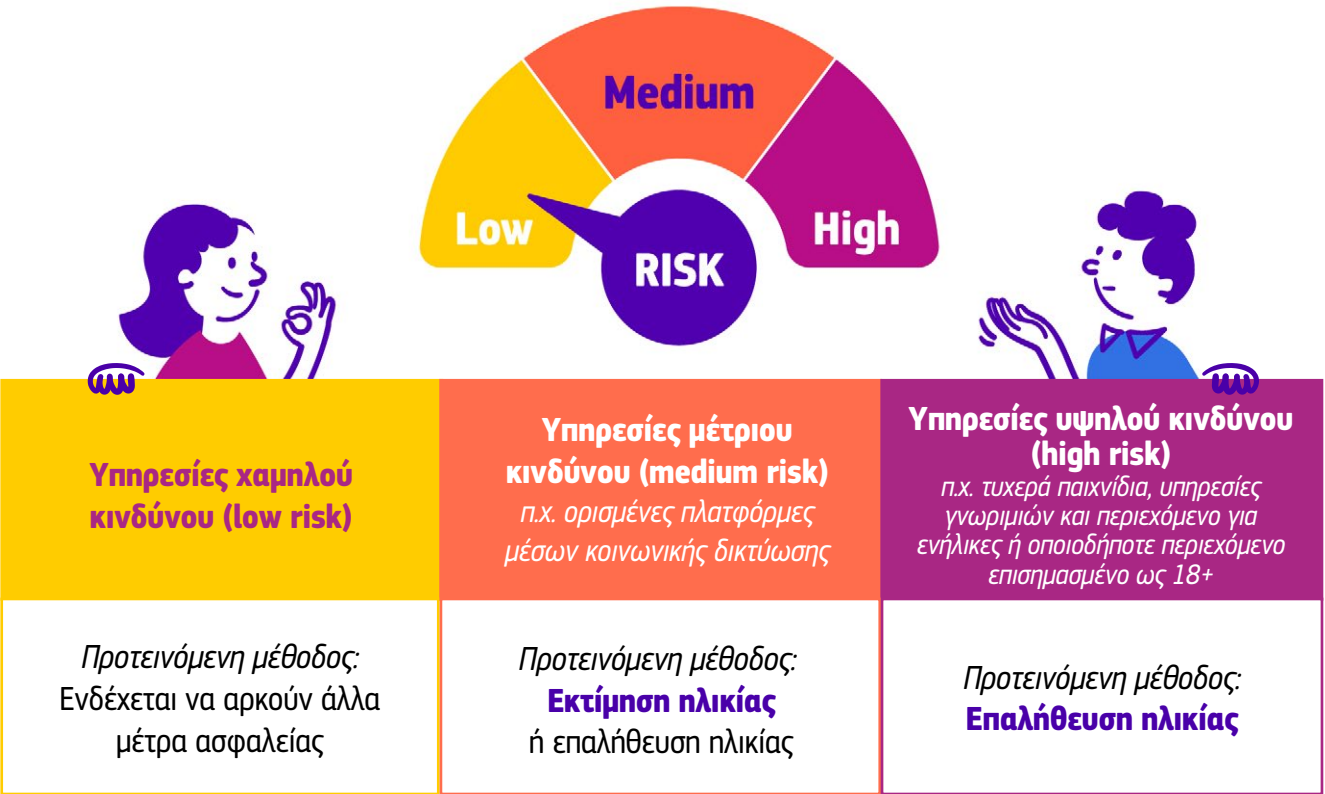
3. Συστάσεις

Οι επιγραφικές πλατφόρμες θα πρέπει:

- ▶ να εξηγούν τον τρόπο ελέγχου της ηλικίας με τρόπο **εύκολα κατανοητό** σε παιδιά και εφήβους
- ▶ να ρωτούν την ηλικία ενός χρήστη μόνο όταν είναι **πραγματικά απαραίτητο** για την ασφάλειά του
- ▶ να χρησιμοποιούν την **απλούστερη** αποτελεσματική **μέθοδο** χωρίς να ζητούν περισσότερες πληροφορίες από όσες χρειάζονται
- ▶ να εγγυώνται ότι όλες οι μέθοδοι διασφάλισης της ηλικίας είναι **ακριβείς, δίκαιες και δύσκολο να παρακαμφθούν**
- ▶ να προσφέρουν **πάνω από μία επιλογές** ώστε να μην αποκλείουν κανέναν
- ▶ να επιτρέπουν στους χρήστες να **κάνουν ένσταση** όταν η ηλικία τους δεν έχει εκτιμηθεί σωστά.



Ποιες μεθόδους πρέπει να χρησιμοποιούν οι πλατφόρμες;



Η διασφάλιση ηλικίας φαίνεται κάπως περίπλοκη, σωστά; Αυτός ο οδηγός για τη διασφάλιση ηλικίας μπορεί να σας βοηθήσει να την κατανοήσετε!



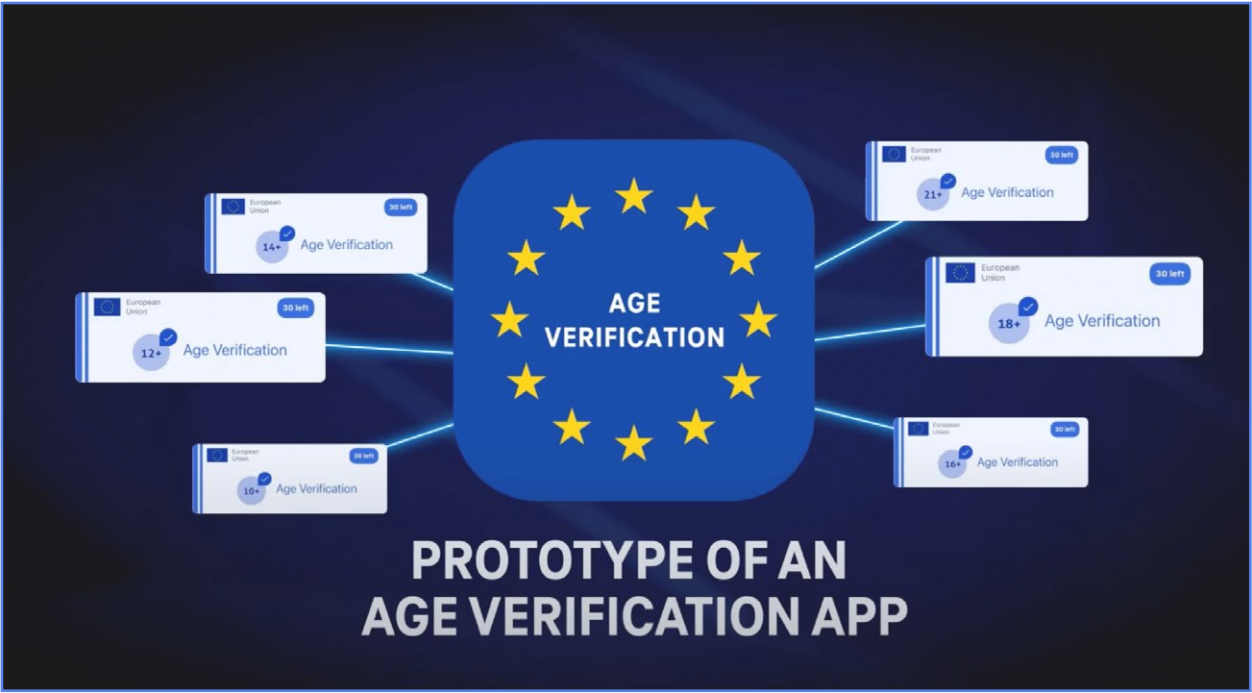
Μπορεί πραγματικά μια εφαρμογή να επαληθεύσει την ηλικία σας;

Ναι! Η Ευρωπαϊκή Επιτροπή προσπαθεί να βρει μια λύση! Τον Ιούλιο του 2025 εγκαινίασε μια **πilotική εφαρμογή επαλήθευσης της ηλικίας**.

Αυτή έχει σχεδιαστεί ώστε:

- ▶ να είναι φιλική προς τον χρήστη
- ▶ να επιτρέπει στους χρήστες να αποδείξουν ότι είναι άνω των 18 ετών
- ▶ να αποφεύγει να ζητά οποιαδήποτε άλλα προσωπικά στοιχεία.

Με τον τρόπο αυτό εξασφαλίζεται ότι η πρόσβαση σε συγκεκριμένο διαδικτυακό περιεχόμενο παραμένει **ασφαλής και κατάλληλη για την ηλικία του χρήστη**.



Θέλετε να μάθετε περισσότερα για την προσέγγιση της ΕΕ για την επαλήθευση ηλικίας; Σαρώστε τον κωδικό QR για περισσότερες πληροφορίες!



3. Συστάσεις

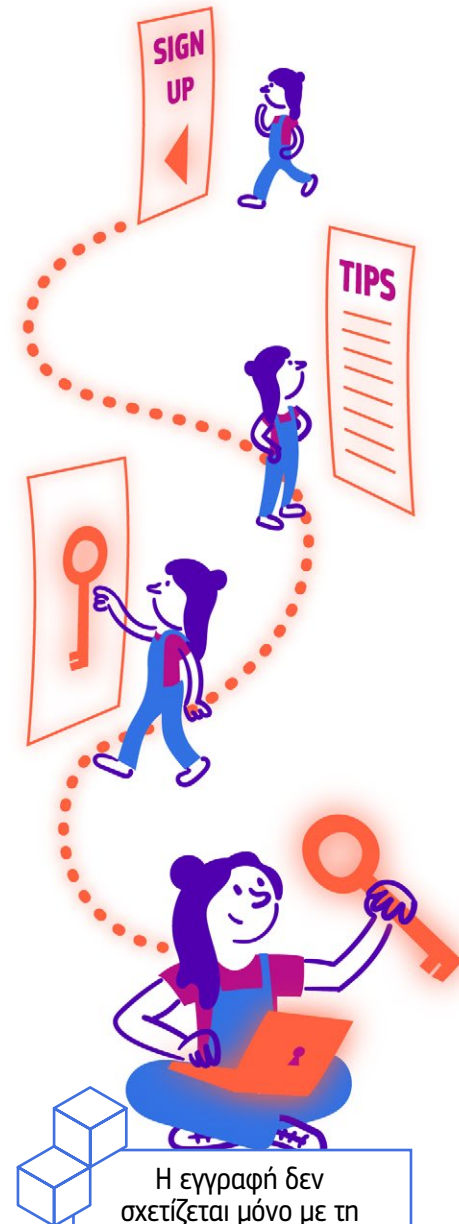
γ. Εγγραφή: πληροφόρηση και ενδυνάμωση από το πρώτο βήμα

Όταν μια πλατφόρμα ζητά από τους χρήστες να εγγραφούν, συχνά είναι μια καλή ευκαιρία για:

- ▶ να κοινοποιήσει στους χρήστες σημαντικές πληροφορίες ασφαλείας·
- ▶ να τους δώσει εκπαιδευτικές συμβουλές·
- ▶ να διασφαλίσει είναι ηλικιακά αρκετά μεγάλοι ώστε να έχουν πρόσβαση.

Για να τα κάνουν όλα αυτά σωστά, οι πλατφόρμες πρέπει:

- ▶ να εξηγούν με σαφήνεια γιατί απαιτείται εγγραφή και ποια είναι τα οφέλη·
- ▶ να διατηρούν τη διαδικασία απλή και προσβάσιμη, ειδικά για παιδιά και εφήβους με πρόσθετες ανάγκες προσβασιμότητας ή αναπηρία·
- ▶ να μην ενθαρρύνουν την εγγραφή σε χρήστες κάτω από ένα συγκεκριμένο ηλικιακό όριο·
- ▶ να διευκολύνουν τα παιδιά και τους εφήβους να αποσυνδεθούν ή να διαγράψουν τον λογαριασμό τους ανά πάσα στιγμή·
- ▶ να χρησιμοποιούν την εγγραφή για να εισάγουν και να εξηγούν στους χρήστες βασικά χαρακτηριστικά ασφαλείας όπως:
 - > ρυθμίσεις απορρήτου,
 - > προεπιλεγμένα μέτρα προστασίας,
 - > εργαλεία υποβολής αναφορών·
- ▶ να βοηθούν τα παιδιά και τους εφήβους να κατανοήσουν:
 - > ποια μέσα ασφαλείας είναι διαθέσιμα,
 - > πώς να αναζητήσουν βοήθεια εάν χρειαστεί.



Η εγγραφή δεν σχετίζεται μόνο με τη δημιουργία ενός λογαριασμού. Αποτελεί και μια ευκαιρία για την πλατφόρμα να διασφαλίσει ότι οι νέοι χρήστες που ξεκινούν τώρα να τη χρησιμοποιούν παραμένουν ασφαλείς και ενημερωμένοι και διατηρούν τον έλεγχο.

δ. Ρυθμίσεις λογαριασμού: πώς να ελέγχετε την ιδιωτικότητα και την ασφάλειά σας

Οι ρυθμίσεις λογαριασμού μπορούν να βοηθήσουν τα παιδιά, τους εφήβους και τους γονείς τους να διαχειριστούν την παρουσία τους στο διαδίκτυο — ελέγχοντας π.χ. πόσα προσωπικά στοιχεία τους είναι ορατά σε άλλους ή πόσο εύκολο είναι να έρθουν άλλοι σε επαφή μαζί τους.

Καθώς οι περισσότεροι άνθρωποι δεν αλλάζουν τις προεπιλεγμένες ρυθμίσεις λογαριασμού, οι πλατφόρμες οφείλουν να εξασφαλίζουν ότι οι ρυθμίσεις αυτές είναι **απόρρητες, ασφαλείς και προστατευμένες εξ αρχής**.

Στις προεπιλεγμένες ρυθμίσεις θα πρέπει να περιλαμβάνονται:

- ▶ **Ο περιορισμός των επαφών:** να ελέγχεται ποιος μπορεί να ακολουθήσει ή να στείλει μήνυμα στο παιδί ή στον έφηβο.
- ▶ **Η απενεργοποίηση επικίνδυνων χαρακτηριστικών** από προεπιλογή, π.χ.:
 - > εντοπισμός θέσης·
 - > αυτόματη αναπαραγωγή βίντεο·
 - > μικρόφωνο και κάμερα·
 - > συγχρονισμός επαφών·
 - > παρακολούθηση.
- ▶ **Η αποτροπή αγνώστων** από την παρακολούθηση ή τη λήψη περιεχομένου.
- ▶ **Ο διαμοιρασμός των στοιχείων επικοινωνίας** (όπως η διεύθυνση email και ο αριθμός τηλεφώνου) **μόνο με ρητή άδεια**.
- ▶ **Η διαχείριση ειδοποιήσεων:** να απενεργοποιούνται **οι ειδοποιήσεις αυτόματης προώθησης (push notifications) ή οι επείγουσες ειδοποιήσεις (alerts)** από συγκεκριμένους χρήστες ή εφαρμογές ή κατά τις ώρες του ύπνου.
- ▶ **Η μείωση της υπερβολικής χρήσης** μέσω της απενεργοποίησης χαρακτηριστικών όπως:
 - > likes («μου αρέσει») και αντιδράσεων·
 - > στοιχείων όπως το «Ο/Η... πληκτρολογεί»·
 - > της λειτουργίας «Διαβάστηκε».
- ▶ **Η προστασία της ψυχικής υγείας:** να απενεργοποιούνται τα φίλτρα εικόνας που ενδέχεται να επηρεάζουν αρνητικά την εικόνα του σώματος ή την αυτοεκτίμηση.



3. Συστάσεις

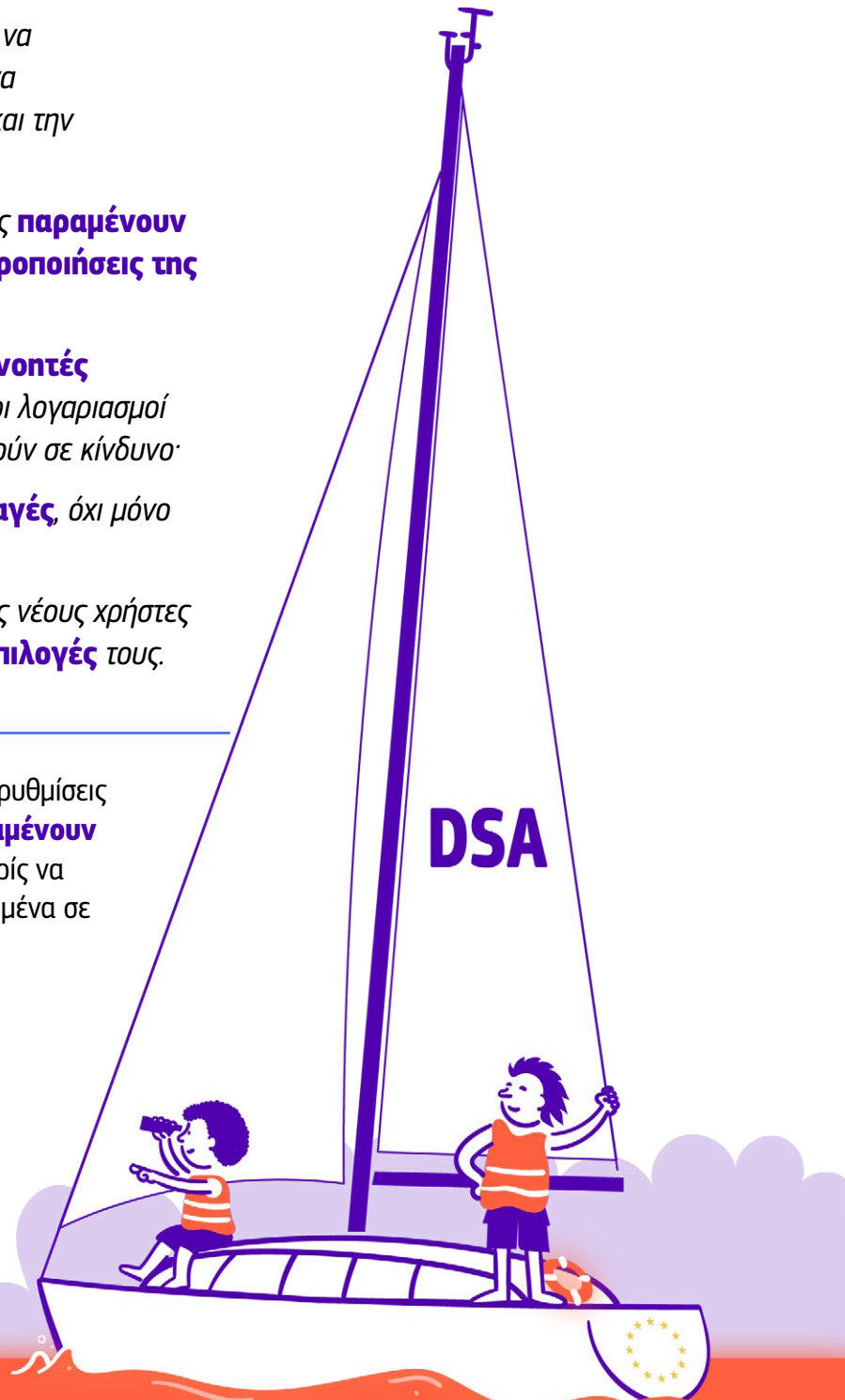
Παραχώρηση του ελέγχου στα παιδιά και στους εφήβους, αλλά με καθοδήγηση

Τα παιδιά δεν θα πρέπει ποτέ να παρακινούνται να μειώσουν τις ρυθμίσεις ιδιωτικότητας, ασφάλειας και προστασίας. Εάν όμως επιθυμούν να **εξατομικεύσουν την εμπειρία τους**, θα πρέπει να μπορούν να το κάνουν με τρόπο ασφαλή και κατάλληλο για την ηλικία τους.

Οι πλατφόρμες θα πρέπει:

- ▶ να επιτρέπουν στους νέους χρήστες να προσαρμόσουν τις ρυθμίσεις ώστε να ανταποκρίνονται στην **ηλικία** τους και την **ωριμότητά** τους·
- ▶ να βεβαιώνονται ότι οι επιλογές τους **παραμένουν ίδιες ακόμη και μετά από επικαιροποιήσεις της πλατφόρμας**·
- ▶ να παρέχουν σαφείς, **εύκολα κατανοητές προειδοποιήσεις** πριν καταστούν οι λογαριασμοί τους λιγότερο ιδιωτικοί ή πριν βρεθούν σε κίνδυνο·
- ▶ να επιτρέπουν **προσωρινές αλλαγές**, όχι μόνο μόνιμες·
- ▶ να ζητούν κατά διαστήματα από τους νέους χρήστες να **επιβεβαιώνουν σημαντικές επιλογές** τους.

Γιατί είναι σημαντικό αυτό: οι προεπιλεγμένες ρυθμίσεις βοηθούν τα παιδιά και τους εφήβους να **παραμένουν ασφαλή και να διατηρούν τον έλεγχο**, χωρίς να αισθάνονται υπερβολικά φορτισμένα ή εκτεθειμένα σε αναίτιους κινδύνους.



ε. Διεπαφές: σχεδιάζοντας εύχρηστες και ασφαλείς πλατφόρμες

Διεπαφή είναι το πώς εμφανίζεται και λειτουργεί μια επιγραμμική πλατφόρμα, δηλαδή αυτό που βλέπετε στην οθόνη σας και ο τρόπος που αλληλεπιδράτε μαζί του. Μια καλά σχεδιασμένη διεπαφή μπορεί να βοηθήσει παιδιά και εφήβους να **παραμένουν ασφαλείς, να αισθάνονται σιγουριά και να απολαμβάνουν τον χρόνο τους στο διαδίκτυο**.

Προκειμένου να αποτρέπουν την υπερβολική χρήση και τις εθιστικές συμπεριφορές, αλλά και για να διευκολύνουν την αποσύνδεση του χρήστη, οι πλατφόρμες θα πρέπει να αποφεύγουν χαρακτηριστικά όπως:

- ▶ απεριόριστη κύλιση («σκρολάρισμα») —όταν η σελίδα φτάνει μέσω κύλισης στο κάτω μέρος της, να ανανεώνεται αυτόματα με νέο περιεχόμενο·
- ▶ λειτουργία «σύρετε για ανανέωση»·
- ▶ διαρκείς ειδοποιήσεις·
- ▶ αυτόματη αναπαραγωγή βίντεο·
- ▶ μηχανισμοί καθημερινής επιβράβευσης, «σερί» (streaks) ή πόντοι που ωθούν τα παιδιά να χρησιμοποιούν την εφαρμογή ή το παιχνίδι σε καθημερινή βάση.



Οι πλατφόρμες θα πρέπει να περιλαμβάνουν:

- ▶ εργαλεία που βοηθούν τα παιδιά και τους εφήβους να **διαχειρίζονται τον χρόνο τους στο διαδίκτυο**, όπως φιλικές υπενθυμίσεις για διαλείμματα·
- ▶ ρυθμίσεις ασφαλείας, καθώς και εργαλεία υποβολής αναφορών και ανατροφοδότησης τα οποία οι νέοι χρήστες θα είναι **εύκολο να εντοπίσουν, να κατανοήσουν και να χρησιμοποιήσουν**·
- ▶ **προσβασιμότητα** για όλους, μεταξύ άλλων και για παιδιά και εφήβους με αναπηρία ή πρόσθετες ανάγκες·
- ▶ σαφείς προειδοποιήσεις όταν τα παιδιά και οι έφηβοι αλληλεπιδρούν με **εργαλεία τεχνητής νοημοσύνης (TN)**.



3. Συστάσεις

στ. Συστήματα συστάσεων και λειτουργίες αναζήτησης: βοηθώντας τα παιδιά να διατηρούν τον έλεγχο

Αναρωτηθήκατε ποτέ πώς οι εφαρμογές που χρησιμοποιείτε ως μέσα κοινωνικής δικτύωσης ή οι αγαπημένες σας πλατφόρμες με τηλεοπτικά προγράμματα γνωρίζουν πάντοτε τι να σας δείξουν στη συνέχεια; Τα **συστήματα συστάσεων** αποφασίζουν τι είδους προτάσεις περιεχομένου ή επαφών θα εμφανιστούν στη ροή περιεχομένου των χρηστών —ακόμη και στις σελίδες εξερεύνησης— ανάλογα με τις αντιδράσεις «μου αρέσει» (likes) του χρήστη, καθώς και ανάλογα με το τι έχει παρακολουθήσει, τι έχει επιλέξει ή τι έχει αποφασίσει να ακολουθεί στο παρελθόν.

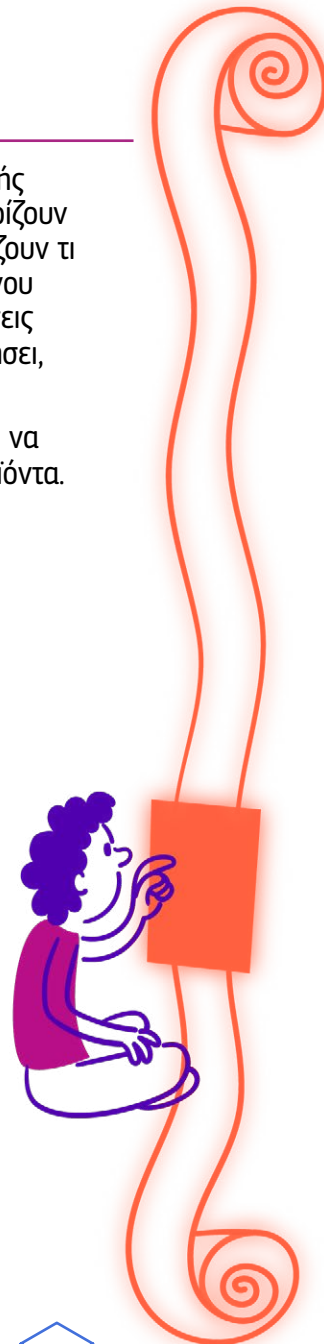
Παρότι αυτό είναι χρήσιμο, μπορεί να οδηγήσει τα παιδιά και τους εφήβους στο να βλέπουν επιβλαβείς ή ακατάλληλες εικόνες, βίντεο, αναρτήσεις ή εμπορικά προϊόντα.

Οι πλατφόρμες θα πρέπει:

- ▶ να δείχνουν μόνο περιεχόμενο κατάλληλο για την ηλικία του χρήστη·
- ▶ να περιορίζουν την ποσότητα των δεδομένων που συλλέγονται και χρησιμοποιούνται για τις συστάσεις·
- ▶ να δίνουν προτεραιότητα στις ενεργές επιλογές και στην ανατροφοδότηση του χρήστη, όπως:
 - > «Δείξε μου λιγότερα/περισσότερα»,
 - > «Δεν θέλω να το βλέπω»,
 - > «Δεν με ενδιαφέρει»·
- ▶ να **μη βασίζονται υπερβολικά στην παθητική ανατροφοδότηση**, π.χ. στον χρόνο παρακολούθησης ή περιήγησης·
- ▶ να εξηγούν **γιατί προτάθηκε κάτι** και πώς μπορούν οι χρήστες να αλλάξουν τη σύσταση·
- ▶ να επιτρέπουν στους χρήστες να **επαναφέρουν τη ροή περιεχομένου τους** πλήρως και οριστικά·
- ▶ να διευκολύνουν την **αναφορά ανεπιθύμητου περιεχομένου** και να εγγυώνται ότι η ανατροφοδότηση του χρήστη αλλάζει πραγματικά το περιεχόμενο που του εμφανίζεται·
- ▶ να κάνουν όλες τις ρυθμίσεις του συστήματος συστάσεων **φιλικές προς τα παιδιά και προσβάσιμες**.

Οι λειτουργίες αναζήτησης θα πρέπει:

- ▶ να αποκλείουν επισφαλείς λέξεις ή hashtag·
- ▶ να βοηθούν τα παιδιά και τους εφήβους να επιλέξουν τι τους ενδιαφέρει περισσότερο.



Τα συστήματα συστάσεων πρέπει να ενδυναμώνουν τα παιδιά, όχι να τα κατακλύζουν με περιεχόμενο. Το να δίνουμε στους νέους χρήστες τη δυνατότητα να ελέγχουν τι βλέπουν τους βοηθά να δημιουργήσουν **πιο ασφαλείς και θετικές εμπειρίες στο διαδίκτυο**.

ζ. Εμπορικές πρακτικές: βοηθώντας τους νέους να κατανοήσουν τι προωθείται και πωλείται

Τα παιδιά και οι έφηβοι —ακριβώς όπως και οι ενήλικες— μπορεί να μη συνειδητοποιούν πάντοτε ότι κάτι είναι:

- ▶ διαφήμιση·
- ▶ έμμεση προωθητική κίνηση·
- ▶ επί πληρωμή ανάρτηση κάποιου influencer.

Μπορεί επίσης να δυσκολεύονται να αντιληφθούν τον τρόπο με τον οποίο οι εφαρμογές, τα παιχνίδια ή οι ιστότοποι προσπαθούν να μας πείσουν να ξοδέψουμε περισσότερο χρόνο ή χρήματα. Αυτό μπορεί να μας οδηγήσει σε περιττές αγορές, υπερβολικές δαπάνες ή σε συνήθειες που είναι δύσκολο να κοπούν. Οι πλατφόρμες θα πρέπει:

- ▶ να επισημαίνουν κάθε είδους διαφημιστικό και χορηγούμενο περιεχόμενο με σαφήνεια και συνέπεια —ακόμη και τις **τοποθετήσεις προϊόντων** των influencers·
- ▶ να επανεξετάζουν τακτικά τις επισημάνσεις των διαφημίσεων και να ελέγχουν ότι οι επισημάνσεις αυτές είναι **ξεκάθαρες και αποτελεσματικές** για τα παιδιά και τους κηδεμόνες τους·
- ▶ να αποφεύγουν να διαφημίζουν σε παιδιά και εφήβους προϊόντα και υπηρεσίες που θα μπορούσαν να βλάψουν **την ιδιωτικότητα, την ασφάλεια ή/και την προστασία τους**·
- ▶ να μοιράζονται ξεκάθαρα στοιχεία σχετικά με τα κόστη και τις συνέπειες που προκύπτουν από:
 - > **αγορές εντός εφαρμογών,**
 - > **εικονικά νομίσματα ή μάρκες,**
 - > άλλες **συναλλαγές**
- ▶ να αποφεύγουν τακτικές πίεσης όπως:
 - > **αντίστροφη μέτρηση,**
 - > μηνύματα τύπου **«αγόρασε τώρα»**·
- ▶ να αποκλείουν την πρόσβαση σε οποιαδήποτε λειτουργία μοιάζει με **τυχερά παιχνίδια**, όπως τα **σεντούκια θησαυρού**·
- ▶ να διασφαλίζουν ότι τα «δωρεάν» προϊόντα και υπηρεσίες δεν περιλαμβάνουν κρυφές αγορές·
- ▶ να εγγυώνται ότι οι διαφημίσεις είναι **κατάλληλες για την ηλικία των χρηστών**·
- ▶ να προσαρμόζουν τους αλγόριθμους έτσι ώστε **τα παιδιά να μην εκτίθενται σε διαφημίσεις για πολλή ώρα ή υπερβολικά συχνά**.

Γιατί είναι σημαντικό αυτό: αυτά τα μέτρα μπορούν να βοηθήσουν στην προστασία των παιδιών και των εφήβων ώστε να μην **εξαπατώνται ή πιέζονται** να ξοδέψουν χρήματα χωρίς να το θέλουν.



Τι σημαίνουν αυτοί οι όροι;

Τοποθέτηση προϊόντος είναι όταν εμφανίζεται μια εμπορική ονομασία ή ένα προϊόν σε ένα βίντεο ή ανάρτηση στο πλαίσιο προώθησης επί πληρωμή.

Σεντούκι θησαυρού (loot box) είναι ένα ψηφιακό αντικείμενο που δίνει τυχαίες ανταμοιβές και χρησιμοποιείται συχνά σε παιχνίδια.

Αγορά εντός εφαρμογής είναι κάτι που αγοράζεις μέσα σε μια εφαρμογή, όπως π.χ. επιπλέον λειτουργίες, περισσότερες ζωές, νέες εμφανίσεις για άβαταρ ή εικονικά νομίσματα.

3. Συστάσεις

η. Έλεγχος περιεχομένου: ασφάλεια και σεβασμός στις πλατφόρμες

Έλεγχος περιεχομένου είναι **η εποπτεία και η αφαίρεση περιεχομένου ή χρηστών** που θα μπορούσαν να βλάψουν την ιδιωτικότητα, την ασφάλεια και την προστασία των παιδιών και των εφήβων, μεταξύ άλλων και τη συνολική σωματική και ψυχική τους ευημερία.

Πρόκειται για ένα σημαντικό μέτρο που στοχεύει στην προστασία των χρηστών και την πρόληψη σοβαρών κινδύνων όπως ο εκφοβισμός, η έκθεση σε επιβλαβές περιεχόμενο ή η αθέμιτη προσέγγιση ανηλίκων (όταν κάποιος προσπαθεί να γίνει φίλος με ένα παιδί ή έναν έφηβο / μια έφηβη ώστε να τον/την ξεγελάσει ή να τον/την κάνει να νιώσει άβολα).

Οι πλατφόρμες θα πρέπει:

- ▶ να ορίζουν ξεκάθαρα τι σημαίνει **επιβλαβές περιεχόμενο και επιβλαβείς συμπεριφορές**·
- ▶ να εφαρμόζουν μια αποτελεσματική διαδικασία ώστε να **αφαιρούν εγκαίρως επιβλαβές ή παράνομο περιεχόμενο και λογαριασμούς**·
- ▶ να εκπαιδεύουν τους επόπτες περιεχομένου ώστε να **εντοπίζουν απειλές για παιδιά και εφήβους, όπως η αθέμιτη προσέγγιση ανηλίκων ή οι επικίνδυνες προκλήσεις**·
- ▶ να αφαιρούν παράνομο ή επιβλαβές περιεχόμενο **χωρίς καθυστέρηση**·
- ▶ να χρησιμοποιούν εργαλεία που θα **εμποδίζουν τους χρήστες να παράγουν ή να διαμοιράζονται επιβλαβές περιεχόμενο που έχει δημιουργηθεί με ΤΝ**·
- ▶ να επανεξετάζουν και να βελτιώνουν τακτικά τον τρόπο με τον οποίο λειτουργούν τα συστήματά τους για τον έλεγχο περιεχομένου.

Ο κατάλληλος έλεγχος περιεχομένου βοηθά να δημιουργηθεί ένας χώρος όπου τα παιδιά και οι έφηβοι **θα αισθάνονται ασφάλεια και θα νιώθουν ότι τα σέβονται και τα υποστηρίζουν**.



Ο έλεγχος περιεχομένου δεν αφορά μόνο την αφαίρεση περιεχομένου —αφορά τη δημιουργία ενός ασφαλέστερου και με περισσότερο σεβασμό διαδικτυακού χώρου για όλους.

θ. Υποβολή αναφορών: διευκολύνοντας τους ανηλίκους να μιλήσουν και να αναζητήσουν βοήθεια

Μερικές φορές στο διαδίκτυο κάτι μπορεί να πάει στραβά. Μπορεί να δείτε κάτι που θα σας αναστατώσει, να υποστείτε εκφοβισμό ή να νιώσετε ανασφάλεια. Για τον λόγο αυτό, είναι σημαντικό οι πλατφόρμες να εξασφαλίζουν πως θα είναι **εύκολο για όλους να αναφέρουν προβλήματα και να αναζητήσουν βοήθεια**.

Οι πλατφόρμες θα πρέπει:

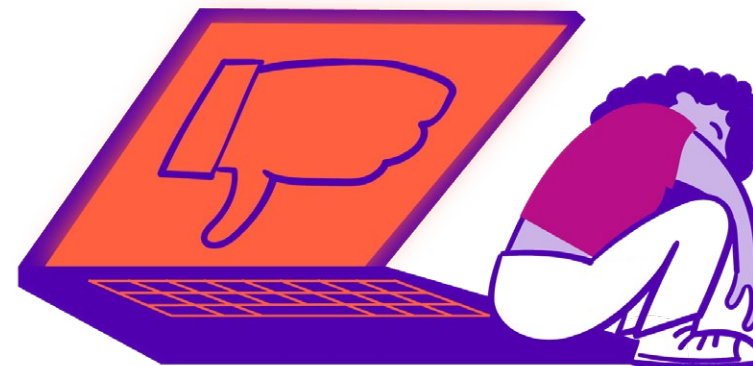
- ▶ να προσφέρουν σε κάθε χρήστη **απλούς και ξεκάθαρους τρόπους αναφοράς** της κακοποίησης, του εκφοβισμού ή του επιβλαβούς περιεχομένου (μεταξύ άλλων και σε άτομα με αναπηρία)·
- ▶ να επιτρέπουν στους χρήστες **να αποκλείουν, να βάζουν σε σίγαση ή να περιορίζουν** σχόλια και αλληλεπιδράσεις με άλλους χρήστες·
- ▶ να διασφαλίζουν ότι οι χρήστες δεν **προστίθενται αυτόματα σε ομάδες**, αλλά μόνο μετά την αποδοχή σχετικής πρόσκλησης·
- ▶ να προσφέρουν **γρήγορες και βοηθητικές** απαντήσεις σε χρήστες που αναφέρουν κάποιο πρόβλημα και να δίνουν ανατροφοδότηση για το τι συνέβη.



Χρειάζεστε βοήθεια για να αναφέρετε ανησυχητικό περιεχόμενο;

Το δίκτυο των Κέντρων Ασφαλούς Διαδικτύου σε ολόκληρη την Ευρώπη μπορεί να σας βοηθήσει!

Ό,τι κι αν είναι αυτό για το οποίο νιώθετε την ανάγκη να μιλήσετε, θα σας προσφέρουν υποστήριξη, πρακτική βοήθεια, καθοδήγηση και θα σας ακούσουν με προσοχή.



3. Συστάσεις

1. Εργαλεία για γονείς και κηδεμόνες

Οι γονείς και οι κηδεμόνες μπορούν να βοηθήσουν τα παιδιά και τους εφήβους να παραμείνουν ασφαλείς στο διαδίκτυο. Οι πλατφόρμες μπορούν να προσφέρουν εργαλεία που υποστηρίζουν αυτόν τον ρόλο, **χωρίς να στερούν από τους νέους τα δικαιώματά τους ή την ανεξαρτησία τους**.

Εάν οι πλατφόρμες επιλέξουν εργαλεία γονικού ελέγχου συμπληρωματικά προς τις υποχρεωτικές ρυθμίσεις ασφαλείας τους, αυτά τα εργαλεία θα πρέπει:

- ▶ να βασίζονται **στην επικοινωνία και στην ενδυνάμωση**, όχι στον έλεγχο·
- ▶ να **σέβονται την ιδιωτικότητα παιδιών και εφήβων** και να τους ειδοποιούν όταν ένας γονέας ή κηδεμόνας ενεργοποιεί τέτοια εργαλεία·
- ▶ να λειτουργούν **σε όλες τις συσκευές και εκδόσεις λογισμικού**·
- ▶ να είναι συμβατά με τα **υπάρχοντα εργαλεία γονικού ελέγχου**, όπως αυτά που είναι ενσωματωμένα σε τηλέφωνα ή εφαρμογές.



Τα εργαλεία για γονείς και κηδεμόνες μπορούν να βοηθήσουν τις οικογένειες να χτίσουν σχέσεις **εμπιστοσύνης και υποστήριξης**, αλλά δεν πρέπει σε καμία περίπτωση να αποτελούν μέσα παρακολούθησης, ούτε να παραβιάζουν τα δικαιώματα των παιδιών. Επίσης, δεν θα πρέπει να αντικαθιστούν τα ενσωματωμένα χαρακτηριστικά ασφαλείας της πλατφόρμας.



Χρειάζεστε υποστήριξη ως γονέας ή κηδεμόνας; Στην **Better Internet for Kids (BIK) Parent Corner** θα βρείτε συμβουλές για να βοηθήσετε τα παιδιά σας να χτίσουν υγιείς ψηφιακές συνήθειες και να μάθουν να περιηγούνται με ασφάλεια στον κόσμο του διαδικτύου.

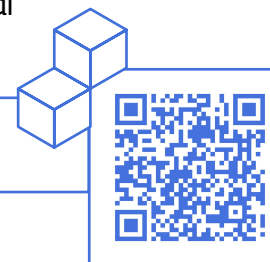


4. Ποιος εξασφαλίζει ότι τηρούνται οι κανόνες της DSA;

Κάθε χώρα της ΕΕ διαθέτει **Συντονιστή Ψηφιακών Υπηρεσιών** [Digital Services Coordinator (DSC)] ο οποίος, σε συνεργασία με την Ευρωπαϊκή Επιτροπή, επιβλέπει και παρακολουθεί πώς εφαρμόζεται η DSA από τις πλατφόρμες.



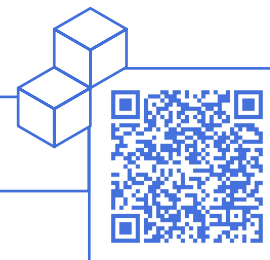
Σαρώστε τον κωδικό QR για να μάθετε ποιος είναι ο DSC στη χώρα σας.



Κάθε DSC μπορεί να διορίσει οργανισμούς που εξειδικεύονται στην ταυτοποίηση και την επισήμανση παράνομου και επιβλαβούς περιεχομένου. Οι οργανισμοί αυτοί αποκαλούνται **αξιόπιστες πηγές επισήμανσης παράνομου περιεχομένου**, και όταν κρούουν τον κώδωνα του κινδύνου, οι πλατφόρμες οφείλουν να δρουν άμεσα! Φανταστείτε τους ως διαιτητές που σφυρίζουν για να επισημάνουν κάποιο πρόβλημα αμέσως μόλις το εντοπίσουν.



Σαρώστε τον κωδικό QR για να μάθετε ποιες είναι οι αξιόπιστες πηγές επισήμανσης παράνομου περιεχομένου στη χώρα σας.



5. Τι θα συμβεί στη συνέχεια;

Η Ευρωπαϊκή Επιτροπή και τα κράτη μέλη της ΕΕ θα εξακολουθήσουν να διασφαλίζουν ότι οι πλατφόρμες τηρούν την DSA και να περιφρουρούν την ασφάλεια των παιδιών και των νέων στο διαδίκτυο. Ήδη συνεργάζονται με τους εξής τρόπους:

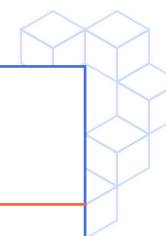
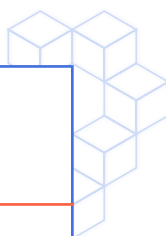
- ▶ ελέγχουν εάν οι πλατφόρμες τηρούν τις κατευθυντήριες γραμμές για την προστασία των ανηλίκων σύμφωνα με την DSA και προχωρούν σε νομικές ενέργειες όταν διαπιστώνονται παραβάσεις·
- ▶ δοκιμάζουν και αναπτύσσουν την **εφαρμογή επαλήθευσης ηλικίας της ΕΕ**·
- ▶ καταρτίζουν ένα **σχέδιο δράσης της ΕΕ κατά του κυβερνοεκφοβισμού**·
- ▶ αναλύουν με ποιους τρόπους **μπορεί να επηρεάσει την ψυχική υγεία η χρήση των μέσων κοινωνικής δικτύωσης** από παιδιά και εφήβους.

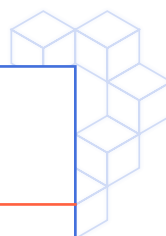


Ηλικία ψηφιακής συναίνεσης

Η ηλικία στην οποία μπορείτε να ξεκινήσετε να χρησιμοποιείτε διαδικτυακές υπηρεσίες χωρίς να χρειάζεστε συναίνεση γονέα. Συνήθως είναι ανάμεσα στα 13 και τα 18 έτη, ανάλογα με το τι ορίζουν οι νόμοι της χώρας σας, αλλά και ανάλογα με τον τύπο υπηρεσίας.







Πού μπορείτε να βρείτε περισσότερες πληροφορίες και βοήθεια;

Πλήρες κείμενο των
κατευθυντήριων γραμμών της
DSA για την προστασία των
ανηλίκων



Ιστότοπος «Better Internet for Kids»



Είτε είστε παιδί ή έφηβος, είτε γονέας, κηδεμόνας ή εκπαιδευτικός, μπορείτε να επικοινωνήσετε με το Κέντρο Ασφαλούς Διαδικτύου της χώρας σας για να λάβετε υποστήριξη ή πληροφορίες για οποιοδήποτε θέμα σχετικά με το διαδίκτυο.

Πάντοτε θα υπάρχει κάποιος διαθέσιμος να σας βοηθήσει — μέσω **τηλεφώνου, ηλεκτρονικού ταχυδρομείου ή ζωντανής συνομιλίας**— και είναι **δωρεάν!**



Αυτό το φυλλάδιο, το οποίο είναι κατάλληλο για όλη την οικογένεια, εξηγεί με απλά λόγια τις κατευθυντήριες γραμμές της Ευρωπαϊκής Επιτροπής για την προστασία των ανηλίκων στο πλαίσιο του νόμου για τις ψηφιακές υπηρεσίες. Δείχνει πώς οι διαδικτυακές πλατφόρμες πρέπει να προστατεύουν τα παιδιά και τους εφήβους, θέτοντας τα δικαιώματά τους σε πρώτη προτεραιότητα, ενσωματώνοντας την προστασία της ιδιωτικής ζωής και την ασφάλεια στον σχεδιασμό της πλατφόρμας, ελέγχοντας την ηλικία των χρηστών, καθιστώντας τις ρυθμίσεις ιδιωτικές, σχεδιάζοντας ασφαλείς διεπαφές, ελέγχοντας το επιβλαβές περιεχόμενο, διευκολύνοντας την αναφορά παραβάσεων και υποστηρίζοντας τους γονείς.

Ευρωπαϊκή Επιτροπή
Γενική Διεύθυνση Επικοινωνιακών Δικτύων, Περιεχομένου και
Τεχνολογίας
Ημερομηνία σύνταξης: Οκτώβριος 2025

Η παρούσα έκδοση είναι ενημερωτική και δεν αποτελεί νομικό έγγραφο.
Λουξεμβούργο: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης, 2025
© Ευρωπαϊκή Ένωση, 2025



Η πολιτική της Επιτροπής για την περαιτέρω χρήση διέπεται από την απόφαση 2011/833/ΕΕ της Επιτροπής, της 12ης Δεκεμβρίου 2011, για την περαιτέρω χρήση εγγράφων της (ΕΕ L 330 της 14.12.2011, σ. 39, ELI: <http://data.europa.eu/eli/dec/2011/833/oj>). Εάν δεν ορίζεται διαφορετικά, η περαιτέρω χρήση του παρόντος εγγράφου επιτρέπεται βάσει της άδειας Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>). Αυτό σημαίνει ότι επιτρέπεται η περαιτέρω χρήση εφόσον αναφέρεται η πηγή και επισημαίνονται οι τυχόν αλλαγές.

Κατεβάστε αυτό το
φυλλάδιο από τη διεύθυνση:
<https://link.europa.eu/cgyKch>



PDF ISBN 978-92-68-31205-6 KK-01-25-130-EL-N doi:10.2759/6901008
Print ISBN 978-92-68-31206-3 KK-01-25-130-EL-C doi:10.2759/2149366



Υπηρεσία Εκδόσεων
της Ευρωπαϊκής Ένωσης

DSA for YOUTH

The Digital Services Act (DSA) explained

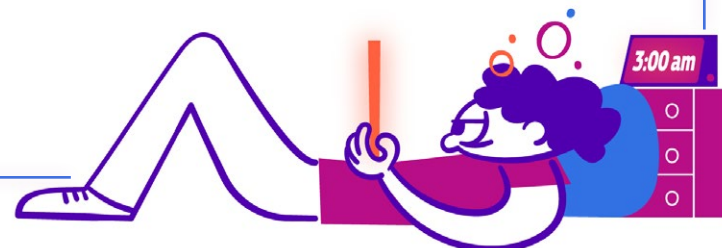
**What online platforms
should do to keep
kids and teens safe online**



What is the Digital Services Act (DSA)?

Online platforms are a big part of everyday life for children and teenagers, whether it's for meeting friends, watching videos, playing games or learning something new. But being online also comes with serious risks. Kids and teens might:

- ▶ be cyberbullied
- ▶ be contacted by strangers with bad intentions
- ▶ see harmful or upsetting content that makes them feel uncomfortable, scared or disturbed
- ▶ feel pressured to buy things
- ▶ participate in dangerous challenges
- ▶ find it hard to put the phone down or switch off the console.



To help make the internet safer, in 2022 the European Union (EU) created the Digital Services Act (DSA). This law applies to online platforms (European or not) available in the EU. It aims to help keep all internet users – including kids and teens – safe from these and other risks, and protect fundamental rights online.

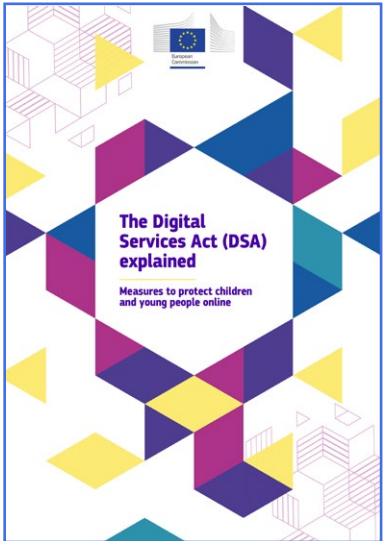
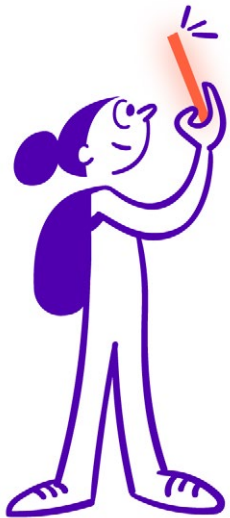
All online platforms must follow this law and help keep users safe in the EU



How does the DSA keep kids and teens safe?

The DSA says that **online platforms must ensure a high level of privacy, safety, and security for minors when they use their services**. This means that children and teenagers should feel protected and safe when they use apps, social media and games that are covered by the law. The largest platforms, which have more than 45 million users in the EU, like TikTok, Instagram and Snapchat, must also identify and assess other potential risks for children and teenagers who use their services.

In July 2025, the European Commission published guidelines on the protection of minors to help all platforms understand what they should do to keep kids and teens safe online. This booklet explains how the guidelines work.



Do you want to learn more about the DSA? Check out this booklet, explaining the measures to protect kids and teens online

Here's what's inside

1. Who has to follow the guidelines on the protection of minors?	4
2. What are the key principles?	5
3. Recommendations	6
a. Risk assessment: every platform comes with different risks	6
b. Age assurance: how platforms check your age	6
c. Registration: information and empowerment from the start	10
d. Account settings: privacy and safety you can control	11
e. Interfaces: designing platforms to be easy and safe to use	13
f. Recommender systems and search features: helping kids stay in control	14
g. Commercial practices: helping kids and teens understand what's being promoted and sold	15
h. Moderation: keeping platforms safe and respectful	16
i. Reporting: making it easy to speak up and get help	17
j. Tools for parents and guardians	18
4. Who makes sure the DSA rules are followed?	19
5. What happens next?	19
Where can you get more information and help?	24

Please note that this publication is intended for information purposes and does not constitute a legal document.

1. Who has to follow the guidelines on the protection of minors?

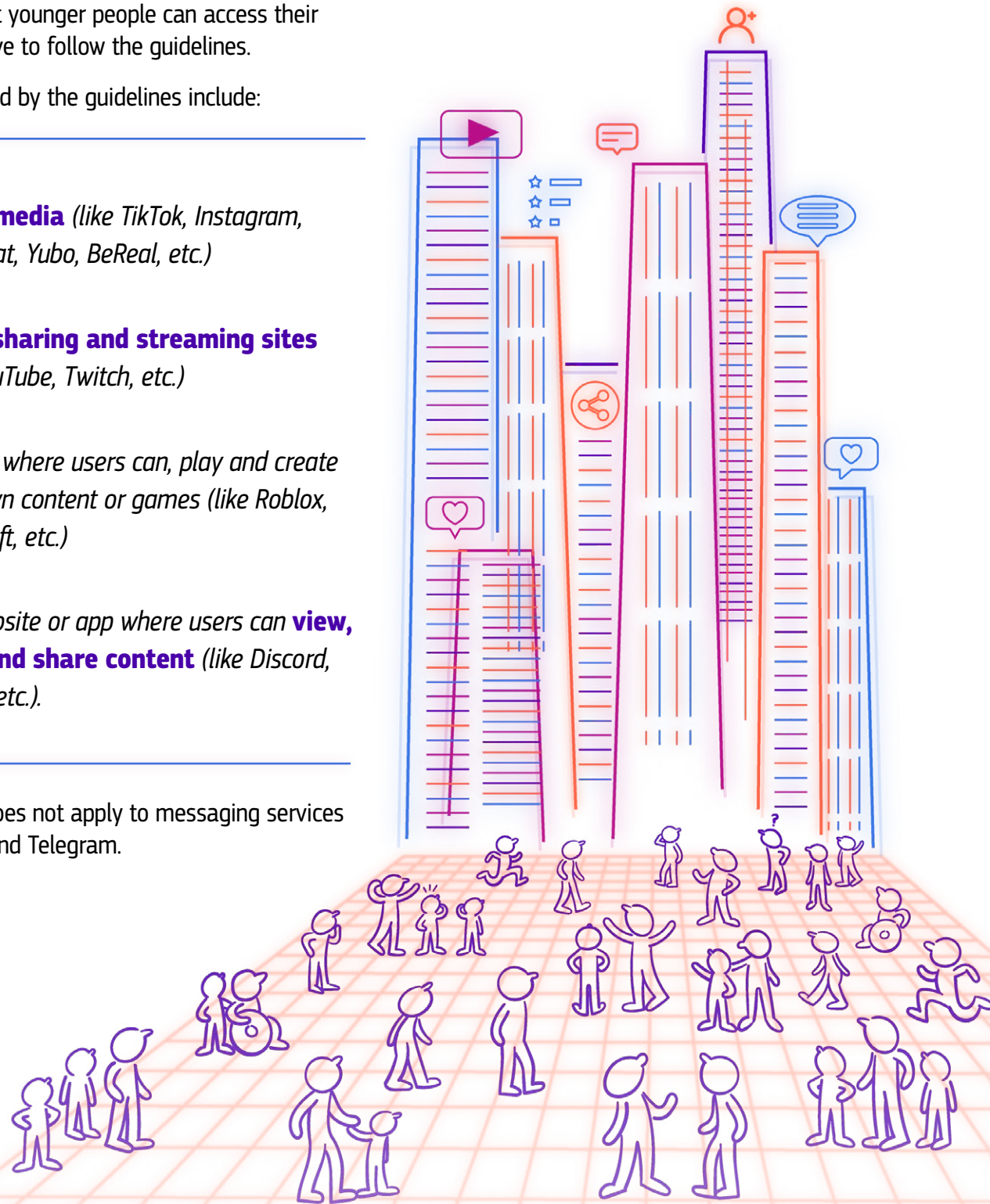
If a platform is used by kids and teens – or if it's likely they may access it – then the platform **must** follow the DSA rules and the guidelines on the protection of minors.

Websites made for grown-ups can't just say 'kids are not allowed' in their rules and ignore what's really happening. If they know that younger people can access their content, they have to follow the guidelines.

Platforms covered by the guidelines include:

- ▶ **social media** (like TikTok, Instagram, Snapchat, Yubo, BeReal, etc.)
- ▶ **video-sharing and streaming sites** (like YouTube, Twitch, etc.)
- ▶ **games** where users can, play and create their own content or games (like Roblox, Minecraft, etc.)
- ▶ **any website or app where users can view, post, and share content** (like Discord, Reddit, etc.).

Note: The DSA does not apply to messaging services like Messenger and Telegram.



2. What are the key principles?

The guidelines are built on three main ideas:

1. Children's rights come first

Platforms should respect children's rights and always act in the child's best interests. These rights include:

- ▶ *protection*
- ▶ *non-discrimination*
- ▶ *inclusion*
- ▶ *privacy*
- ▶ *access to information and education*
- ▶ *freedom of expression*
- ▶ *participation.*



This means designing, developing, and operating platforms that are always *safe, private, and secure*.

2. Safety by design

Platforms should not wait for problems to happen. They should build privacy, safety and security into their services from the start. Features should be appropriate for different ages and stages of children's development.

3. Understanding the needs of users

Platforms need to carefully consider how their services are used by children and teenagers, and what risks they might face, such as:

- ▶ *cyberbullying*
- ▶ *harmful content*
- ▶ *excessive use.*



Then, they must find solutions to reduce those risks.

3. Recommendations

Let's take a look at the recommendations that online platforms need to follow to protect kids and teens online.

a. Risk assessment: every platform comes with different risks

The guidelines recommend that platforms should **regularly check** whether their services pose **risks to kids and teens** and understand how and why. They need to find the right balance between:

- ▶ letting kids and teens share their content, ideas and thoughts
 - ▶ giving them the chance to explore, play and learn new things online...
- ... while keeping them safe!

Once risks are identified, platforms should respond with effective solutions – without limiting the important opportunities and benefits that children and teenagers can enjoy online.

b. Age assurance: how platforms check your age

To make platforms safer – and to prevent kids and teens from using services that are not meant for them – it's important to know whether users are **old enough** to access certain content.

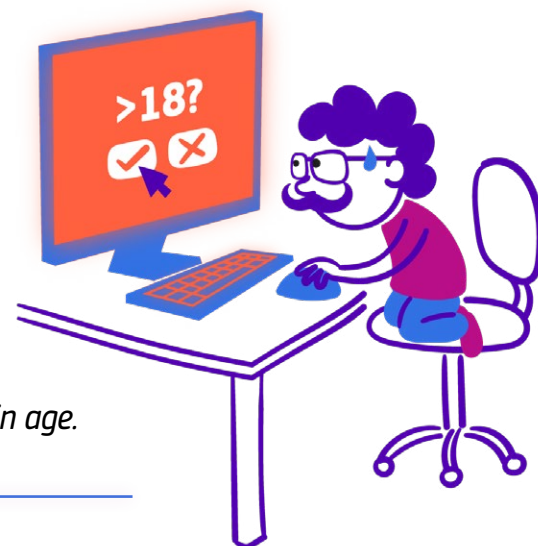
This is where **age assurance** comes in.

Age assurance means using tools to:

- ▶ find out or estimate a user's age, or
- ▶ confirm whether someone is above or below a certain age.

Did you know?

You have to be at least 13 years old to use TikTok, Snapchat, Instagram, BeReal and Steam!



Types of age assurance

There are 3 main ways platforms can check a user's age:

1. Self-declaration

You enter your date of birth, or click 'Yes, I'm over 13' or 'Yes, I'm over 18'. It's quick, but easy to cheat, so it's **not effective nor reliable**.

2. Age estimation

Technology estimates your age based on things like:

- > face scans
- > typing style
- > what you're interested in.

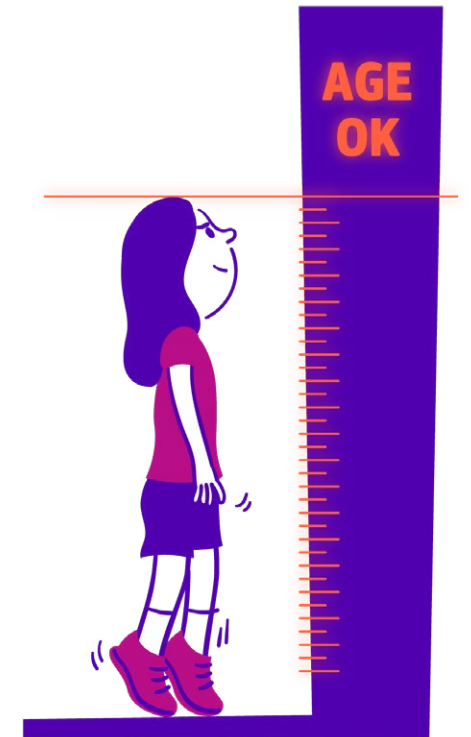
It's not perfect – it can't tell your exact age, and it might be **intrusive** for your privacy.

3. Age verification

This is the **most accurate** method. It checks your age using:

- > official documents, like a passport
- > trusted digital IDs, like an ID issued by the government, or the [EU Digital Identity Wallet](#).

This last method **protects your privacy** because users can prove their age without revealing any other personal data.



What's the [EU Digital Identity Wallet](#)? It's a free app (coming in 2026) that helps people in Europe:

- ▶ keep important documents safe in one place,
- ▶ prove who they are, online and in real life.

It's like a digital backpack for your ID and important papers.



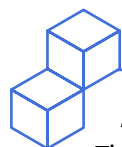
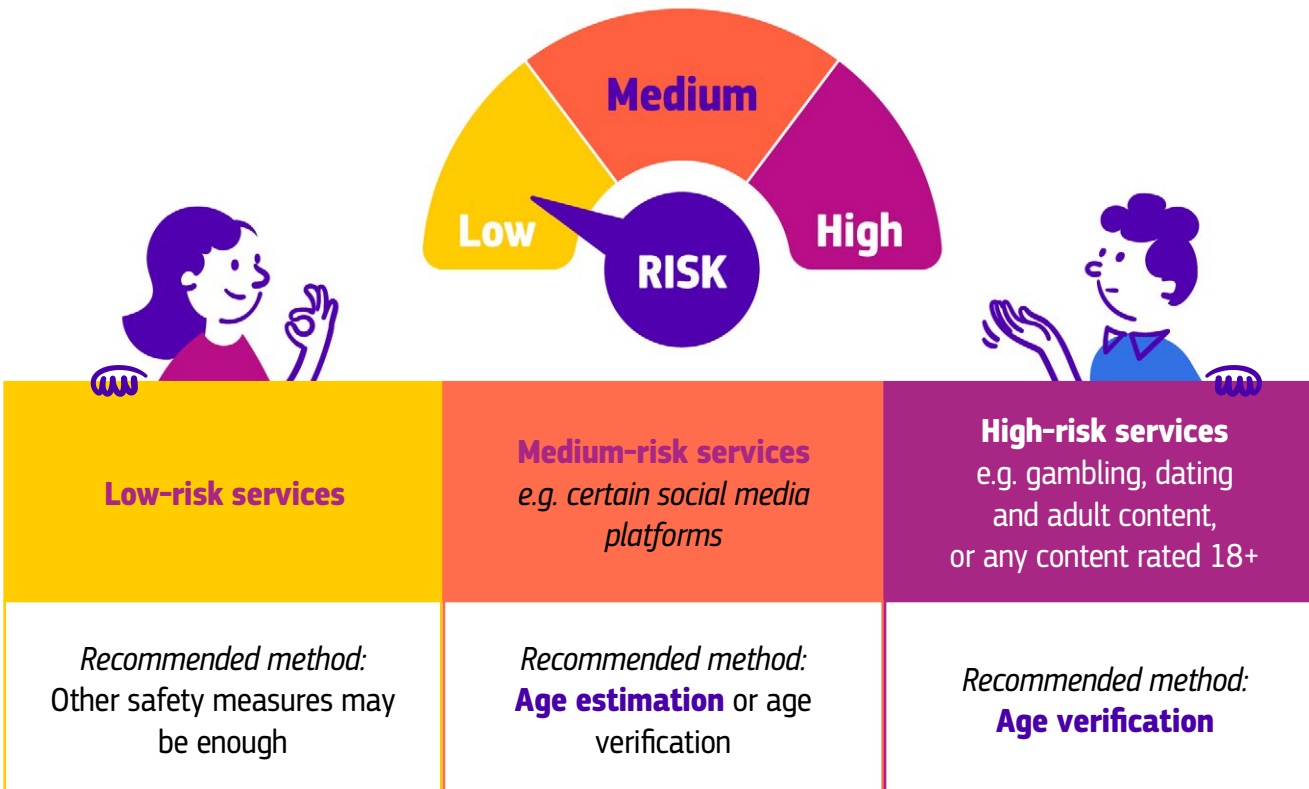
3. Recommendations

Online platforms should:

- ▶ explain age checks in a way that's **easy to understand** for kids and teens
- ▶ only ask about age when it's **really needed** to help keep users safe
- ▶ use the **simplest method** that works well without asking for more information than needed
- ▶ make sure all age assurance methods are **accurate, fair, and hard to bypass**
- ▶ offer **more than one option**, so no one is left out
- ▶ allow users to **appeal** if their age is not estimated correctly.



What method should platforms use?



Age assurance looks a bit complicated, doesn't it?
This [guide to age assurance](#) can help you understand!



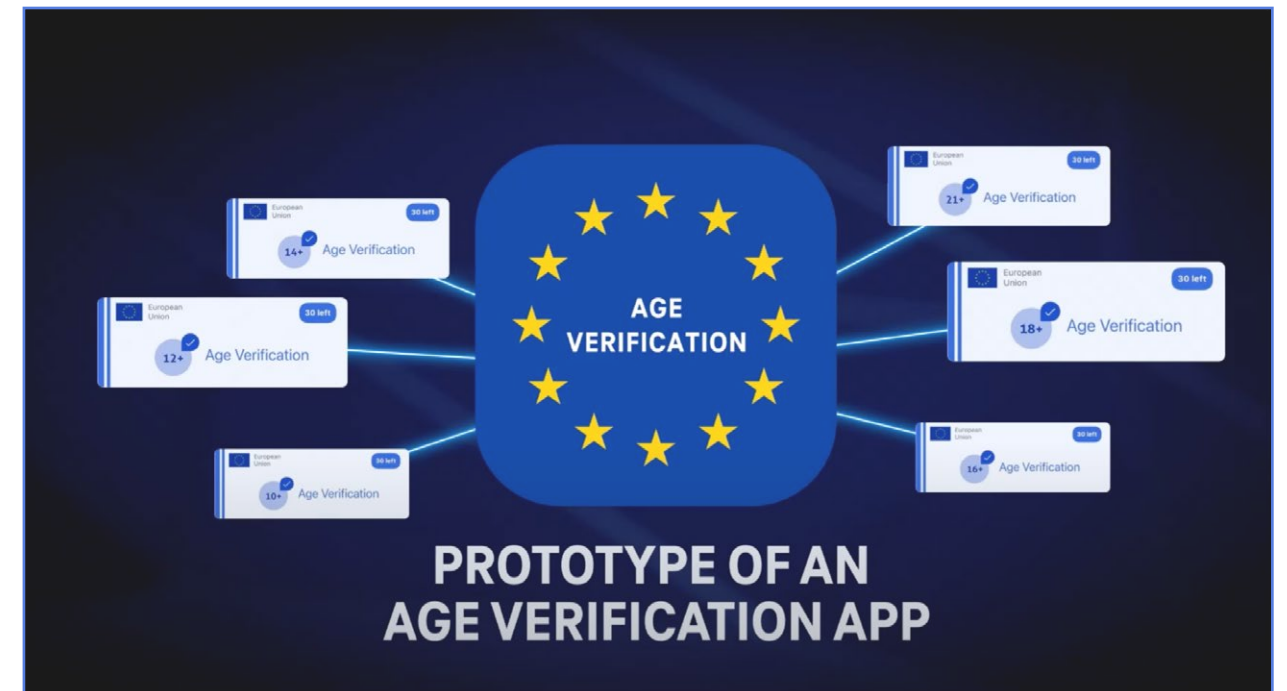
Can an app really verify your age?

Yes! The European Commission is working on a solution for you! In July 2025, it launched a **blueprint for an age-verification app**.

It's designed to:

- ▶ be user-friendly
- ▶ allow users to prove that they are 18 or over
- ▶ avoid asking for any other personal details.

This helps keep access to certain online content **safe and age appropriate**.



Are you curious about the EU's approach to age verification? Scan the QR code to learn more!



3. Recommendations

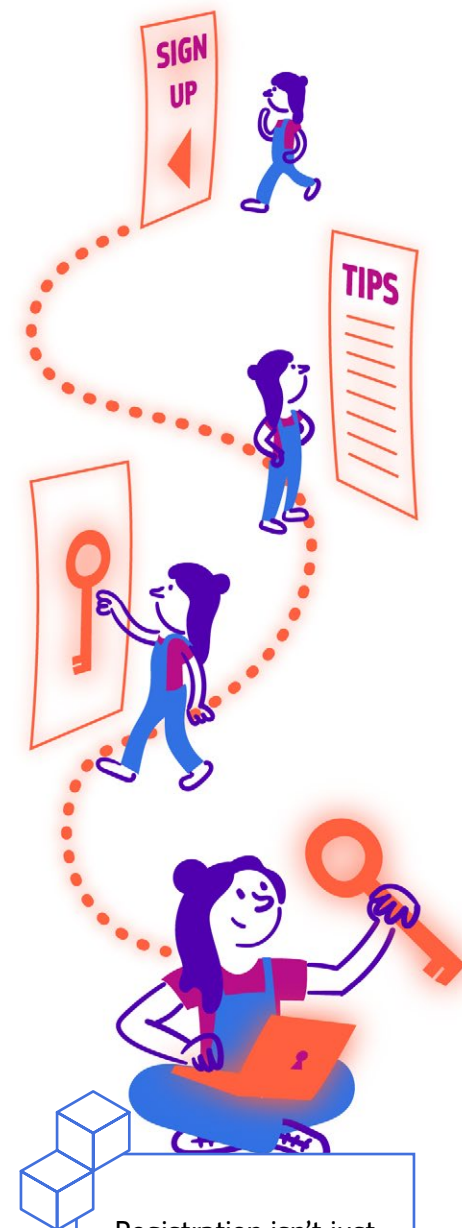
c. Registration: information and empowerment from the start

When a platform asks users to register, it's often a good opportunity to:

- ▶ share important **safety information**
- ▶ provide **educational tips**
- ▶ ensure the user is **old enough** to access.

To do this well, platforms need to:

- ▶ **clearly explain** why registration is needed and what the benefits are
- ▶ keep the **process simple and accessible**, especially for kids and teens with additional needs or disabilities
- ▶ avoid encouraging users who are **too young to sign up**
- ▶ make it easy for children and teens to **log out** or **delete their accounts** at any time
- ▶ use registration to introduce and explain **key safety features** like:
 - > privacy settings
 - > default protections
 - > reporting tools
- ▶ help children and teens understand:
 - > what **safety tools are available**
 - > how to **get help** if needed.



Registration isn't just about creating an account. It's a chance for the platform to make sure young users start off **safe, informed** and **in control**.

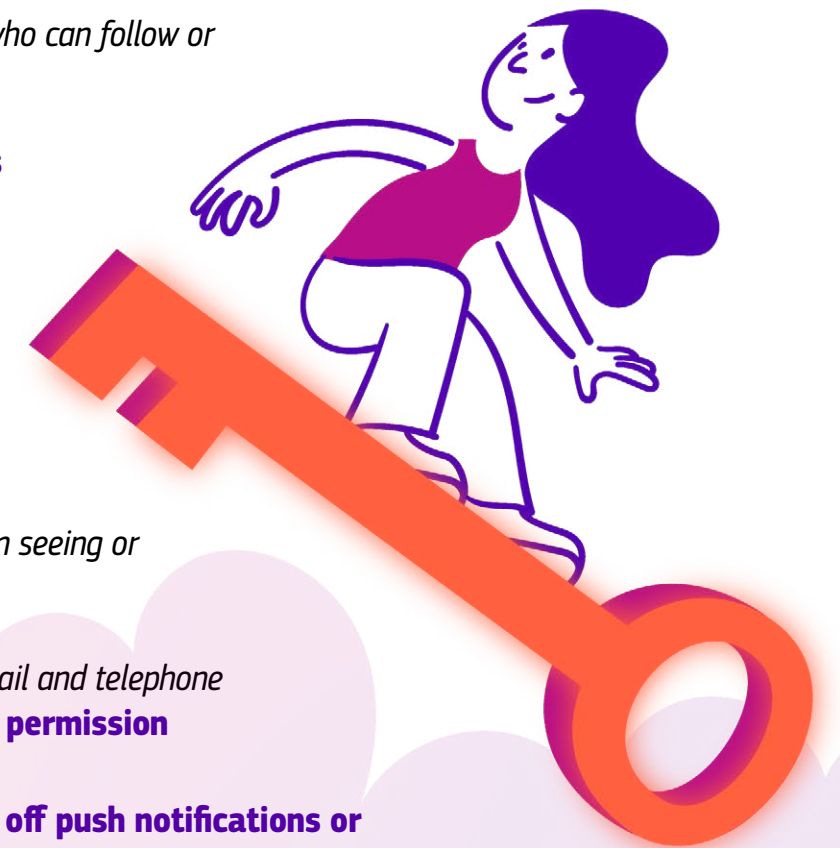
d. Account settings: privacy and safety you can control

Account settings can help children, teenagers and their parents or guardians manage their online presence – like how much personal information is visible to others, or how easy it is to be contacted.

Since most people don't change the default settings, platforms need to make sure these are **private, safe and secure from the start**.

Default settings should include:

- ▶ **Limiting contact:** control who can follow or message the child or teen
- ▶ **Turning off risky features** by default, such as:
 - > geolocation
 - > autoplay of videos
 - > microphone and camera
 - > contact syncing
 - > tracking.
- ▶ **Preventing strangers** from seeing or downloading content
- ▶ Sharing contact info (like email and telephone number) **only with explicit permission**
- ▶ Managing notifications: **turn off push notifications or alerts** from certain users or apps, or during sleep hours
- ▶ Reducing **excessive use** by turning off features like:
 - > likes and reactions counters
 - > "...is typing" features
 - > read receipts.
- ▶ **Protecting mental health:** turn off image filters that may negatively affect body image or self-esteem.



3. Recommendations

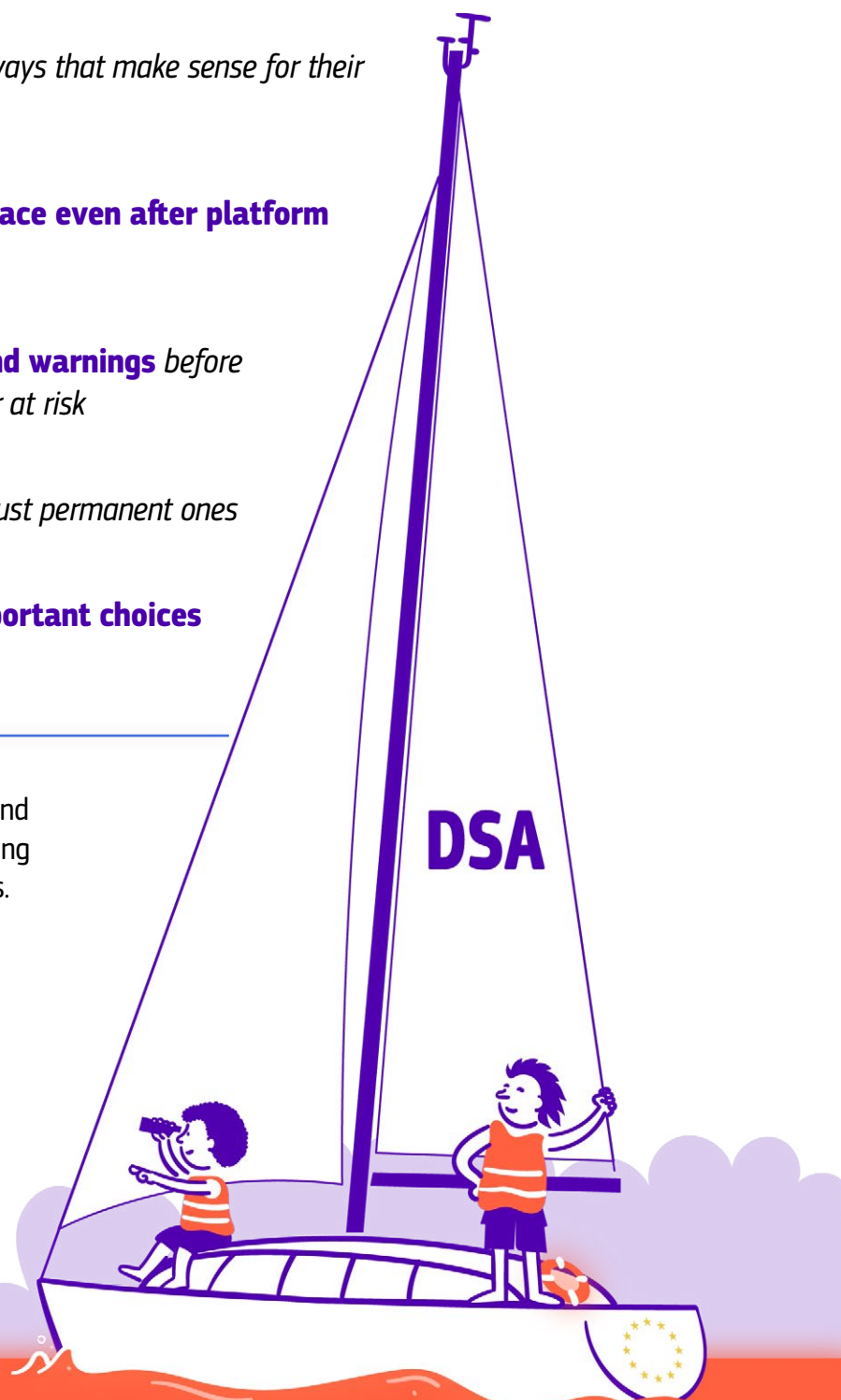
Giving kids and teens control – with guidance

Kids and teens should never be encouraged to lower their privacy, safety and security settings. But if they want to **customise their experience**, they should be able to do so in a way that's safe and age appropriate.

Platforms need to do:

- ▶ let young users adjust settings in ways that make sense for their **age and maturity**
- ▶ make sure their choices **stay in place even after platform updates**
- ▶ provide clear, **easy-to-understand warnings** before making their account more open or at risk
- ▶ **allow temporary changes**, not just permanent ones
- ▶ ask young users to **reconfirm important choices** from time to time.

Why this matters: default settings help kids and teens stay **safe and in control**, without feeling overwhelmed or exposed to unnecessary risks.



e. Interfaces: designing platforms to be easy and safe to use

An **interface** is how an online platform looks and works – what you see on your screen and how you interact with it. A well-designed interface can help kids and teens **stay safe, feel confident** and **enjoy their time online**.

To prevent excessive use and addictive behaviours, and make it easier to log off, platforms should avoid features like:

- ▶ infinite scrolling – when the page has scrolled all the way to the bottom, it automatically refreshes with new content
- ▶ pull to refresh
- ▶ constant notifications
- ▶ video autoplay
- ▶ virtual daily rewards, streaks or points that require children to open the app or game every day.



Platforms need to include:

- ▶ tools that help kids and teens **manage their time online**, like friendly reminders to take breaks
- ▶ safety settings, and reporting and feedback tools that are **easy to find, understand and use**
- ▶ **accessibility** for everyone, including children and teenagers with disabilities or additional needs
- ▶ clear **warnings** when children and teenagers are interacting with **artificial intelligence (AI)** features.



3. Recommendations

f. Recommender systems and search features: helping kids stay in control

Do you ever wonder how your social media apps or your favourite TV shows' platforms always know what to show you next?

Recommender systems decide what kind of content or contact suggestions show up in users' feeds – including explore pages – based on what they've liked, watched, clicked on or decided to follow before.

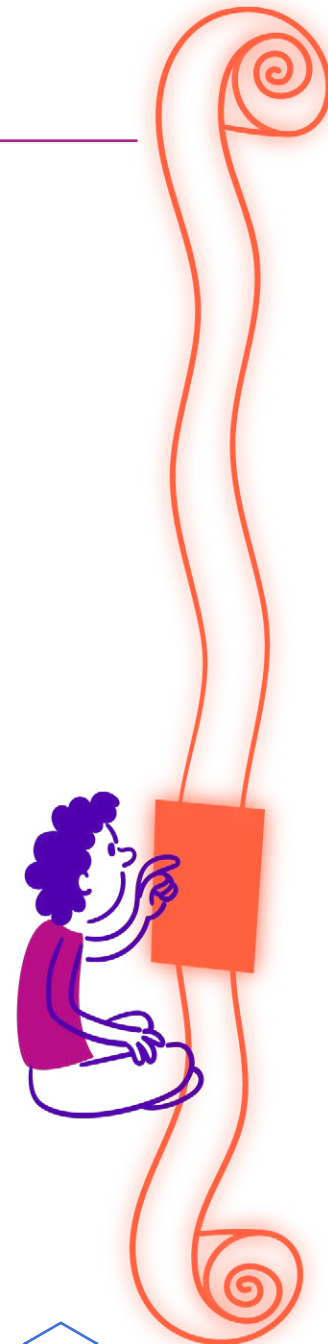
While this can be helpful, it can also lead kids and teens to see harmful or inappropriate images, videos, posts or commercial products.

Platforms should:

- ▶ *only show content that is **age-appropriate***
- ▶ *limit how much **data is collected and used** to make recommendations*
- ▶ *prioritise active **user choices and feedback**, like:*
 - > 'Show me less/more of this'
 - > 'I don't want to see this'
 - > 'I am not interested in this'
- ▶ *avoid relying too much on passive feedback, like how long users watch or browse*
- ▶ *explain **why something was recommended** and how users can change it*
- ▶ *let users **reset their feed** completely and permanently*
- ▶ *make it easy to **report unwanted content** — and ensure feedback actually changes what is shown*
- ▶ *make all recommender system settings **child-friendly and accessible**.*

Search features should:

- ▶ *block unsafe words or hashtags*
- ▶ *help children and teens choose what interests them most.*



Recommender systems should empower kids and teens, not overwhelm them. Giving young users control over what they see helps build **safer, more positive online experiences**.

g. Commercial practices: helping kids and teens understand what's being promoted and sold

Children and teens – just like adults – may not always realise when something online is

- ▶ an advertisement ("ads")
- ▶ a hidden promotion
- ▶ a paid post by an influencer.

It can also be hard to spot how apps, games or websites try to convince us to spend more time or money. This can lead to unnecessary purchases or habits that are hard to break.

Platforms need to:

- ▶ *clearly and consistently label all advertising and sponsored content – including influencers' **product placements***
- ▶ *regularly review how ads are labelled, and check with children and guardians that labels are **clear and effective***
- ▶ *avoid advertising to children and teenagers products and services that could harm **privacy, safety, and/or security***
- ▶ *be transparent about the costs and implications of:*
 - > **in-app purchases**
 - > **virtual currencies or tokens**
 - > other **transactions**.
- ▶ *Avoid pressure tactics like:*
 - > **countdown timers**
 - > **'buy now'** messages.
- ▶ *block access to any feature that resembles **gambling**, like **loot-boxes***
- ▶ *ensure "free" products and services don't include hidden purchases*
- ▶ *make sure advertising is **age-appropriate***
- ▶ *adapt advertising algorithms so **children are not exposed to ads too much or too often**.*

Why this matters to you: these measures can help to protect kids and teens from being **tricked or pressured** into spending money when they don't want to.



What do these terms mean?

A **product placement** is when a brand or item is shown in a video or post as part of a paid promotion.

A **loot box** is a digital item that gives random rewards, often used in games.

An **in-app purchase** is something you buy inside an app, like extra features, more lives, new skins or virtual coins.

3. Recommendations

h. Moderation: keeping platforms safe and respectful

Moderation means **checking and removing content or users** that could harm kids' and teens' privacy, safety and security, including their overall physical and mental well-being.

It's an important tool to protect users and prevent serious risks such as bullying, exposure to harmful content, or grooming (when someone tries to be friends with a child or teen to trick them or make them feel uncomfortable).

Platforms should:



- ▶ clearly define what is meant by **harmful content and behaviours**
- ▶ use an efficient process to **quickly remove harmful or illegal content and accounts**
- ▶ train moderators to spot threats to children and teenagers, such as **grooming or dangerous challenges**
- ▶ remove illegal or harmful content **without delay**
- ▶ use tools to **prevent users from generating or sharing harmful AI content**
- ▶ regularly **review and improve** how moderation systems work.



Good moderation helps create a space where kids and teens feel **safe, respected and supported**.

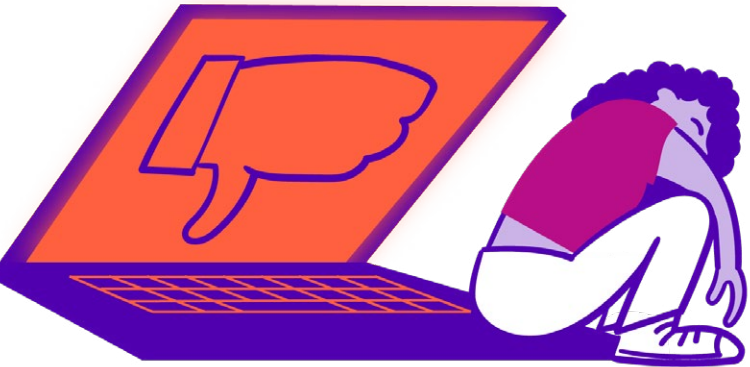
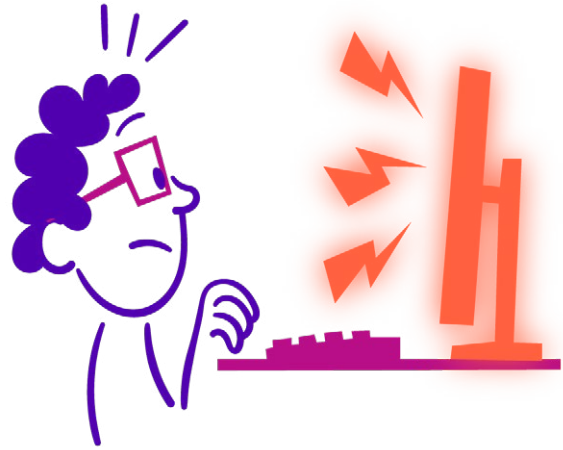
Moderation isn't just about removing content – it's about building a safer, more respectful online space for everyone

i. Reporting: making it easy to speak up and get help

Sometimes things go wrong online. You might see something upsetting, be bullied or feel unsafe. That's why it's important that platforms make it **easy for everyone to report problems and get help**.

Platforms need to:

- ▶ offer **simple and clear ways** for any user to **report** abuse, cyberbullying or harmful content (including persons with disabilities)
- ▶ allow users to **block, mute or restrict** comments and interactions with other users
- ▶ make sure that users aren't **automatically added to groups** – joining should only happen after accepting an invitation
- ▶ provide **fast and helpful responses** when users report a problem and feedback on what happened.



Need help reporting upsetting content?

The network of Safer Internet Centres across Europe can help you!

Whatever you need to talk about, they offer support, practical help, guidance and someone to listen.

3. Recommendations

j. Tools for parents and guardians

Parents and guardians can help children and teens stay safe online. Platforms can offer tools that support this role, **without taking away the young person's rights or independence**.

If platforms choose parental control tools to complement their obligatory safety features, such tools should:

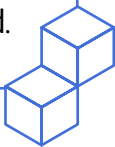
- ▶ be based on **communication and empowerment**, not control
- ▶ **respect children's and teens' privacy**, and notify them when a parent or guardian activates such tools
- ▶ work across **all devices and software versions**
- ▶ be compatible with **existing parental tools**, like the ones built into phones or apps.



Tools for parents and guardians can help families build **trust and support** – but should never result in surveillance or take away a child's rights. They also shouldn't replace the platform's built-in safety features.



Need support as a parent or guardian? The Better Internet for Kids (BIK) Parent Corner offers tips to help your children build good digital habits and safely navigate the online world.

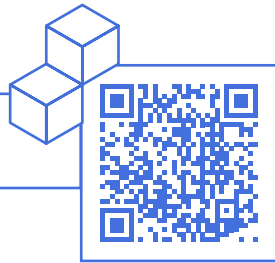


4. Who makes sure the DSA rules are followed?

Each EU country has a **Digital Services Coordinator (DSC)** who works with the European Commission to supervise and monitor how platforms apply the DSA.



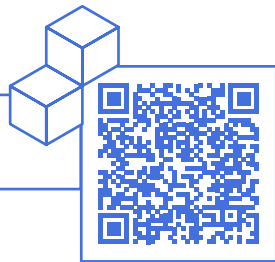
Scan the QR code to find out who the DSC is in your country



Each DSC can appoint organisations that are experts in identifying and flagging illegal and harmful content which are appointed by DSCs. They are called **trusted flaggers**, and when they raise concerns, platforms must act quickly! Think of them as referees who call out problems as soon as they spot them.



Scan the QR code to find out who the trusted flaggers are in your country.



5. What happens next?

The European Commission and EU Member States will continue to make sure platforms follow the DSA and keep children and young people safe online. Together they are:

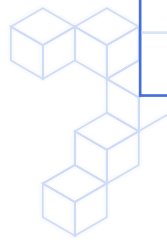
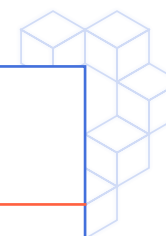
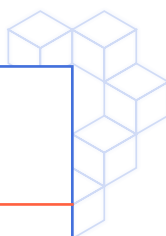
- ▶ checking if platforms follow the guidelines on the protection of minors under the DSA, and starting legal proceedings if they don't
- ▶ testing and rolling out the **EU age-verification app**
- ▶ developing an **EU action plan against cyberbullying**
- ▶ analysing how **social media use can impact mental health** in children and teens.

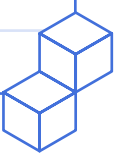
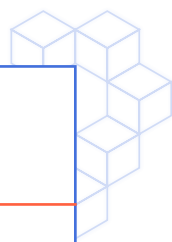


Digital age of majority

The age when you can start using online services on your own — without needing a parent's OK. It's usually 13 or 18, depending on the rules in your country and the type of service.







Where can you get more information and help?

Full text of the DSA guidelines on the protection of minors online



Better Internet for Kids portal



Whether you're a child or teenager, parent, guardian or educator, you can contact the Safer Internet Centre in your country for help or information on any online issue.

Help is always available — by **phone, email, or online chat** – and it's **free!**



This family-friendly booklet explains the European Commission's protection of minors guidelines under the Digital Services Act in simple terms. It shows how online platforms should keep children and teens safe by putting their rights first, integrating privacy and safety in the design of the platform, checking ages, making settings private, designing safe interfaces, moderating harmful content, making reporting easy, and supporting parents – so young people can enjoy the internet with confidence and support.

Directorate-General for Communications Networks,
Content & Technology (DG CONNECT)
Manuscript completed in October 2025

Please note that this publication is intended for information purposes and does not constitute a legal document.
Luxembourg: Publications Office of the European Union, 2025
© European Union, 2025

Download this booklet at:
<https://link.europa.eu/cgyKch>



The Commission's reuse policy is implemented under Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39, ELI: <http://data.europa.eu/eli/dec/2011/833/oj>). Unless otherwise noted, the reuse of this document is authorised under the Creative Commons Attribution 4.0 International (CC BY 4.0) licence (<https://creativecommons.org/licenses/by/4.0/>). This means that reuse is allowed, provided appropriate credit is given and any changes are indicated.

PDF ISBN 978-92-68-31207-0 KK-01-25-130-EN-N doi: 10.2759/7053090

Print ISBN 978-92-68-31208-7 KK-01-25-130-EN-C doi: 10.2759/8280512