MARIA-NEFELI CHRISTODOULOPOULOU
LAWYER | GDPR & AI COMPLIANCE

Σκοπός

Σκοπός του παρόντος άρθρου είναι η ανάλυση της σταδιακής μετάβασης του παραδοσιακού ευρωπαϊκού μοντέλου συγκατάθεσης (“opt-in”) προς global opt-out μηχανισμούς και μια νέα μορφή διαχείρισης προτιμήσεων ιδιωτικότητας μέσω ρυθμιζόμενων αυτοματοποιημένων σημάτων γενικής προτίμησης του χρήστη με δίαυλο τον browser (δίχως τη χρήση cookie banners). Ειδικότερα, εξετάζεται η σύγκρουση μεταξύ του ευρωπαϊκού κανονιστικού πλαισίου του GDPR και της Οδηγίας ePrivacy, το οποίο βασίζεται στην προηγούμενη και ρητή συγκατάθεση του χρήστη (opt-in) prior consent, και του αμερικανικού μοντέλου Opt-Out, το οποίο αναπτύσσεται γύρω από μηχανισμούς opt-out και αντίστοιχα εδράζεται στη φιλοσοφία “Do Not Sell / Share’’, όπως το Global Privacy Control (GPC).

Παράλληλα, το άρθρο επιχειρεί να αποτυπώσει τις πρόσφατες κανονιστικές εξελίξεις σε Ευρωπαϊκή Ένωση και Ηνωμένες Πολιτείες, ιδίως σε σχέση με:
— την κρίση λειτουργικότητας των cookie banners,
— το φαινόμενο του consent fatigue,
— την εμφάνιση των μηχανισμών opt-out ,
— και τη συζήτηση με ρυθμιζόμενες προτιμήσεις μέσω browser από τον χρήστη μέσω αυτοματοποιημένων «σημάτων» ως πιθανής επόμενης γενιάς κανονιστικής συμμόρφωσης της ιδιωτικότητας.

Μέσα από συγκριτική προσέγγιση του ευρωπαϊκού και αμερικανικού

μοντέλου, αναλύονται οι νομικές, τεχνικές και επιχειρησιακές προκλήσεις που δημιουργούνται για οργανισμούς, digital platforms, advertisers και τα τμήματα Κανονιστικής συμμορφώσης, καθώς και τα ανοιχτά ζητήματα σχετικά με τη συμβατότητα των αυτοματοποιημένων privacy signals με τις απαιτήσεις εγκυρότητας της συγκατάθεσης κατά τον GDPR.

Εισαγωγή

Η συζήτηση γύρω από το opt-in και το opt-out αποτελεί σήμερα έναν από τους σημαντικότερους άξονες εξέλιξης του δικαίου προστασίας δεδομένων και της ψηφιακής συμμόρφωσης. Πίσω από τα cookie banners, τα consent management platforms και τα “Accept All” buttons σε κάθε είσοδο του χρήστη σε ιστοσελίδες, αναπτύσσεται μια βαθύτερη σύγκρουση μεταξύ δύο διαφορετικών κανονιστικών φιλοσοφιών: του ευρωπαϊκού μοντέλου προληπτικής συγκατάθεσης (opt-in) και του αμερικανικού μοντέλου μεταγενέστερου δικαιώματος αντίρρησης (opt-out). Στην πραγματικότητα, πίσω από τα cookie banners, τα consent management platforms (CMPs) και τα “Accept All”, κρύβεται μία βαθύτερη κανονιστική και οικονομική αντιπαράθεση: ποιος ελέγχει τα δεδομένα του χρήστη και ποιο είναι το πραγματικό όριο της ψηφιακής αυτονομίας.

Η Ευρωπαϊκή Ένωση αντιμετωπίζει την προστασία προσωπικών δεδομένων ως θεμελιώδες δικαίωμα, κατοχυρωμένο στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της ΕΕ., σε σύγκριση με τις Ηνωμένες Πολιτείες όπου η προστασία ιδιωτικότητας εξελίχθηκε κυρίως μέσα από ένα πλαίο προστασίας των καταναλωτών και τις εκάστοτε Νομοθεσίες Ιδιωτικότητας των Πολιτειών. Η διαφοροποίηση αυτή εξηγεί γιατί το

ευρωπαϊκό σύστημα βασίστηκε επί δεκαετίες στο prior consent model, ενώ το αμερικανικό οικοδόμησε μηχανισμούς μεταγενέστερης άρνησης opt-out ή περιορισμού της επεξεργασίας σε ανίθεση με το πρώτο στο οποίο, η επεξεργασία για σκοπούς tracking, συμπεριφορικής διαφήμισης και non-essential cookies επιτρέπεται μόνο εφόσον ο χρήστης παράσχει προηγούμενη, ελεύθερη, ειδική και εν πλήρει επιγνώσει συγκατάθεση. Η νομική βάση αυτής της αρχής εντοπίζεται κυρίως στο άρθρο 5(3) της Οδηγίας ePrivacy 2002/58/EC, όπως τροποποιήθηκε από την Οδηγία 2009/136/EC, σε συνδυασμό με τα άρθρα 4(11), 6 και 7 GDPR.

Αντίθετα, στις Ηνωμένες Πολιτείες — ιδίως μετά την εμφάνιση του California Consumer Privacy Act (CCPA) και του California Privacy Rights Act (CPRA) — κυριαρχεί το μοντέλο opt-out, δηλαδή, η συλλογή και χρήση δεδομένων επιτρέπεται καταρχήν, εκτός αν ο χρήστης ασκήσει δικαίωμα αντίρρησης ή “Do Not Sell / Share”. Η διαφορά αυτή δεν είναι απλώς τεχνική, είναι δομική και αντικατοπτρίζει δύο διαφορετικές φιλοσοφίες περί ιδιωτικότητας: η Ευρώπη αντιμετωπίζει την προστασία δεδομένων ως θεμελιώδες δικαίωμα (άρθρο 8 Χάρτη Θεμελιωδών Δικαιωμάτων ΕΕ), ενώ οι ΗΠΑ περισσότερο ως ζήτημα προστασίας καταναλωτών και προστασίας από αθέμιτες εμπορικές πρακτικές.

Τα τελευταία δύο χρόνια, ωστόσο, το ευρωπαϊκό μοντέλο βρίσκεται υπό σημαντική πίεση. Η μαζική εμφάνιση consent banners κάθε φορά που οι χρήστες εισέρχονται σε ιστοσελίδες, οδήγησε σε αυτό που πλέον οι ευρωπαϊκές αρχές και η ακαδημαϊκή κοινότητα αποκαλούν “consent fatigue”. Ο χρήστης βομβαρδίζεται καθημερινά με αναδυόμενα παράθυρα συγκατάθεσης, τα οποία στην πράξη συχνά οδηγούν σε μη ουσιαστική συγκατάθεση. Παράλληλα, έρευνες δείχνουν εκτεταμένη χρήση dark patterns στα cookie banners, με interfaces σχεδιασμένα ώστε να ωθούν τον χρήστη στο “Accept All”.

Τα τελευταία χρόνια, όμως, η εικόνα μεταβάλλεται στοιχειωδώς, καθώς η εμφάνιση του **Global Privacy Control (GPC)**, η ενσωμάτωση global opt-out μηχανισμών σε πολιτειακούς νόμους των ΗΠΑ και οι νέες ευρωπαϊκές συζητήσεις γύρω από την αυτόματη αναγνώριση σημάτων από τους

browsers δείχνουν ότι το παραδοσιακό consent banner μοντέλο βρίσκεται πλέον υπό σοβαρή αναθεώρηση.

Το GPC, ένα σύστημα αυτόματης αναγνώρισης σημάτων από τους browsers, που επιτρέπει στον χρήστη να δηλώνει μία γενική προτίμηση opt-out απέναντι στο tracking και στην πώληση δεδομένων θεωρείται σε Πολιτείες όπως η Καλιφόρνια, ήδη νομικά δεσμευτικό για πολλές επιχειρήσεις βάσει του CPRA. Στην Ευρώπη, όμως, η ενσωμάτωσή του δημιουργεί σημαντικά νομικά ερωτήματα.

Μπορεί ένα γενικό browser signal να θεωρηθεί “συγκεκριμένο” και να πληροί τους όρους της “ενημερωμένης και ελεύθερης συγκατάθεσης” κατά GDPR;

Ακριβώς εδώ εντοπίζεται η μεγάλη κανονιστική εξέλιξη του **2025-2026**: η πρόταση της Ευρωπαϊκής Επιτροπής για το **“Digital Omnibus”,** επιχειρεί να ενσωματώσει σημαντικό μέρος των κανόνων του ePrivacy μέσα στον ίδιο τον GDPR μέσω των νέων άρθρων 88a και 88b.

Το προτεινόμενο άρθρο 88b GDPR εισάγει για πρώτη φορά την έννοια των standardized automated privacy signals σε επίπεδο browser ή operating system. Με απλά λόγια, ο χρήστης θα μπορεί να ρυθμίζει μία φορά τις προτιμήσεις ιδιωτικότητας και επεξεργασίας των δεδομενων του στον browser του και οι ιστοσελίδες θα υποχρεούνται να τις αναγνωρίζουν αυτόματα.

Η εξέλιξη αυτή θεωρείται από πολλούς ως μερική μετατόπιση της Ευρώπης προς ένα πιο “opt-out-φιλικό” μοντέλο, καθώς παρότι τυπικά η λογική της συγκατάθεσης παραμένει, πρακτικά η «συγκατάθεση» ενδέχεται να

εκφράζεται πλέον μέσω browser-signals (σημάτων) και όχι μέσω ατομικών banners ανά ιστοσελίδα.

Νομικές αντιρρήσεις

Ορισμένοι φορείς υποστηρίζουν ότι το μοντέλο αυτό υπονομεύει την αρχή της συγκατάθεσης για συγκεκριμένο σκοπό του GDPR και οδηγεί σε μία υπερβολικά γενική μορφή συναίνεσης ή άρνησης. Παράλληλα, κράτη μέλη όπως η Γαλλία έχουν ήδη εκφράσει επιφυλάξεις για τη μεταφορά τεχνικών κανόνων ePrivacy μέσα στον GDPR, θεωρώντας ότι δημιουργείται σύγχυση μεταξύ data protection law και του πλαισίου ηλεκτρονικών επικοινωνιών (ePrivacy framework).

Το σημαντικότερο όμως είναι ότι η ίδια η ΕΕ φαίνεται πλέον να αναγνωρίζει πως το παραδοσιακό consent banner απέτυχε επιχειρησιακά ως προβεβλημένο μοντέλο.

Πρακτικά, σήμερα διαμορφώνονται τρία παράλληλα μοντέλα:

1. Το κλασικό ευρωπαϊκό opt-in model (GDPR + ePrivacy).

1. Το αμερικανικό opt-out model (CCPA/CPRA + GPC).

1. Το αναδυόμενο browser-signal model της ΕΕ μέσω του Digital Omnibus και του άρθρου 88b.

Το τρίτο μοντέλο είναι ίσως η σημαντικότερη εξέλιξη της τελευταίας δεκαετίας στον χώρο της online ρυθμιστικού πλαισίου, διότι επιχειρεί να μεταφέρει τη συγκατάθεση από το επίπεδο της ιστοσελίδας στο επίπεδο του browser ή του λειτουργικού συστήματος.

Νομικά, ωστόσο, παραμένουν ανοικτά κρίσιμα ερωτήματα:

1. **κατά πόσο ένα browser σήμα από τον χρήστη πληροί το άρθρο 7 GDPR,**
2. **ποιος θεωρείται controller για το signal,**
3. **πώς αποδεικνύεται η συγκατάθεση,**
4. **και εάν η αυτοματοποιημένη διαχείριση συγκατάθεσης οδηγεί τελικά σε παράκαμψη της αρχής της «ενημερωμένης συγκατάθεσης» οδηγώντας τον χρήστη σε σύγχυση και ασάφεια ως προς την πληροφόρησή του.**

Η πραγματικότητα είναι ότι η Ευρώπη φαίνεται να μετακινείται σταδιακά από το “consent economy” προς ένα πιο αυτόματο privacy ecosystem. Το αν αυτό θα οδηγήσει σε ουσιαστικότερη προστασία ή απλώς σε νέο τύπο κανονιστικής πολυπλοκότητας, παραμένει ανοιχτό να διευκρινιστεί υπό πραγματικές συνθήκες.

Σε αντίθεση με το ευρωπαϊκό opt-in μοντέλο:

- η συλλογή δεδομένων μπορεί να ξεκινήσει εξαρχής,
- το βάρος μεταφέρεται στον χρήστη να ασκήσει opt-out,
- και η συμμόρφωση εστιάζει περισσότερο στη δυνατότητα άρνησης παρά στην προγενέστερη αδειοδότηση της επεξεργασίας.

Η πρακτική αυτή θεωρήθηκε περισσότερο συμβατή

- με το τεχνολογικό περιβάλλον διαφήμισης ad-tech ,
- τη βιομηχανία συμπεριφορικής διαφήμισης,
- και τη λειτουργία των μεγάλων digital platforms.

Η Εμφάνιση του Global Privacy Control (GPC)

Η σημαντικότερη εξέλιξη των τελευταίων ετών είναι η εμφάνιση του Global Privacy Control (GPC). Το GPC αποτελεί αυτοματοποιημένη παροχή

σήματος μέσω browser με το οποίο ο χρήστης μπορεί να δηλώνει μία γενική προτίμηση opt-out για στοχευμένη διαφήμιση και διαμοιρασμό δεδομένων.

Σε αντίθεση με τα παραδοσιακά cookie banners:
— το GPC λειτουργεί σε επίπεδο browser,
— αποστέλλει αυτόματα privacy signals,
— και επιτρέπει στον χρήστη να εκφράζει μία ενιαία προτίμηση ιδιωτικότητας για πολλαπλές ιστοσελίδες.

Τεχνικά, το signal αποστέλλεται:
— **είτε ως HTTP header,**
— **είτε μέσω JavaScript property προσβάσιμου από το website.**

Το κρίσιμο στοιχείο είναι ότι αρκετές πολιτείες των ΗΠΑ θεωρούν πλέον το GPC νομικά δεσμευτικό global opt-out μηχανισμό.

Πολιτειακή Νομοθεσία στις ΗΠΑ

Η Καλιφόρνια, το Κολοράντο και το Κονέκτικατ έχουν ήδη ενσωματώσει ρυθμίσεις που απαιτούν από τις επιχειρήσεις να αναγνωρίζουν global opt-out signals.

Σύμφωνα με το CPRA όταν ανιχνεύεται GPC signal, η επιχείρηση πρέπει να το αντιμετωπίζει ως έγκυρο αίτημα opt-out, χωρίς να απαιτείται επιπλέον ενέργεια από τον χρήστη.

Αντίστοιχα το Colorado Privacy Act, και το Connecticut Data Privacy Act, επιβάλλουν αυτοματοποιημένη αναγνώριση των global opt-out σημάτων τα οποια δέχονται. Αυτό πρακτικά σημαίνει ότι οι επιχειρήσεις δεν μπορούν πλέον να βασίζονται αποκλειστικά σε cookie banners, αλλά πρέπει να διαθέτουν τεχνικούς μηχανισμούς ανίχνευσης browser privacy signals.

Η Ευρωπαϊκή Κρίση του Consent Banner Model

Παρότι το ευρωπαϊκό opt-in model θεωρείται το αυστηρότερο διεθνώς,

αντιμετωπίζει πλέον σοβαρή κρίση λειτουργικότητας. Η μαζική χρήση cookie banners οδήγησε:
— σε consent fatigue,
— σε banner blindness,
— και σε εκτεταμένη χρήση dark patterns.

Στην πράξη, μεγάλος αριθμός χρηστών:
— αποδέχεται cookies μηχανικά,
— χωρίς πραγματική κατανόηση,
— γεγονός που αμφισβητεί την ουσιαστική εγκυρότητα της συγκατάθεσης.

Ακριβώς λόγω αυτής της αποτυχίας, η Ευρωπαϊκή Επιτροπή εξετάζει πλέον μετατόπιση προς ένα σύστημα το οποίο θα βασίζεται σε προτιμήσεις μέσω αυτοματοποιημένου γενικού σσήματος με δίαυλο τον browser, όπως αναδεικνύουν οι προτεινόμενες ρυθμίσεις του “Digital Omnibus”.

Η προτεινόμενη εισαγωγή των άρθρων 88a και 88b GDPR φαίνεται να ανοίγει τον δρόμο για standardized automated privacy signals εντός της ΕΕ και να δημιουργέι τις κατάλληλες συνθήκες για να προσπελαστού τα εμπόδια των αποτυχημένων μοντέλων.

Εάν η μεταρρύθμιση αυτή προχωρήσει:
— «η συγκατάθεση» ενδέχεται να μεταφερθεί από το επίπεδο του website στο επίπεδο του browser ή του λειτουργικού συστήματος,
— δημιουργώντας ένα υβριδικό μοντέλο μεταξύ ευρωπαϊκού opt-in και αμερικανικού browser-level opt-out .

Συμπέρασμα

Η προτεινόμενη μεταφορά των κανόνων του ePrivacy μέσα στον GDPR μέσω των νέων άρθρων 88a και 88b του Digital Omnibus έχει προκαλέσει σημαντικές επιφυλάξεις σε ορισμένα κράτη μέλη, ιδίως στη Γαλλία. Το βασικό επιχείρημα είναι ότι μέχρι σήμερα το ePrivacy framework προστάτευε αυτοτελώς τον τερματικό εξοπλισμό (υπολογιστές) του χρήστη

και το απόρρητο των ηλεκτρονικών επικοινωνιών, ανεξάρτητα από το εάν υπήρχε επεξεργασία προσωπικών δεδομένων κατά GDPR. Αντίθετα, ο GDPR επικεντρώνεται στη νομιμότητα της επεξεργασίας προσωπικών δεδομένων και στις υποχρεώσεις των controllers. Η ενσωμάτωση των ρυθμιζόμενων στους browser privacy signals στον GDPR θεωρείται ότι ενδέχεται να συγχέει δύο διαφορετικά κανονιστικά αντικείμενα — την προστασία της συσκευής και τη διακυβέρνηση της επεξεργασίας δεδομένων — μεταφέροντας παράλληλα αυξημένη ρυθμιστική ισχύ στους browser παρόχους και στις μεγάλες τεχνολογικές πλατφόρμες, γεγονός το οποίο πλέον δημιουργεί εύλογα ερωτήματα χρήσης εξουσίας (ισχύος) -καθώς και δυνατότητας επίβλεψης υπό την εποπτεία των DPA (αρχών προστασίας), εξουσία η οποία μεταφέρεται πλέον από τις ιστοσελίδες:

— στα operating systems,
— και στις μεγάλες τεχνολογικές πλατφόρμες που ελέγχουν την ίδια την αρχιτεκτονική των προτιμήσεων ιδιωτικότητας, με όσες συνέπειες μπορεί κανείς να υποπτευθεί στο μέλλον της πρόληψης και της καταστολής των παραβιάσεων ιδιωτικότητας.

References

— Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR).
— Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive), as amended by Directive 2009/136/EC.
— Charter of Fundamental Rights of the European Union, Articles 7 and 8.
— Planet49 Judgment.
— European Data Protection Board, Guidelines 05/2020 on Consent under Regulation 2016/679.
— European Data Protection Board, Guidelines 03/2022 on Dark Patterns in Social Media Platform Interfaces.
— California Consumer Privacy Act (CCPA).

— California Privacy Rights Act (CPRA).
— Colorado Privacy Act (CPA).
— Connecticut Data Privacy Act (CTDPA).
— Digital Omnibus Proposal – proposed Articles 88a and 88b GDPR.
— Global Privacy Control (GPC) Technical Specification.

Disclaimer: This document is provided for informational purposes only and does not constitute legal advice.