



Αθήνα, 25/02/2020
Αρ. πρωτ: Γ/ΕΞ/1525/25-02-2020

ΣΥΣΤΑΣΕΙΣ 1/2020

Συμμόρφωση υπευθύνων επεξεργασίας δεδομένων με την ειδική νομοθεσία για τις ηλεκτρονικές επικοινωνίες

Η Αρχή έχει διαπιστώσει σε ικανό βαθμό έλλειψη συμμόρφωσης των παρόχων υπηρεσιών της κοινωνίας της πληροφορίας στις ειδικές απαιτήσεις της νομοθεσίας για την επεξεργασία δεδομένων στις ηλεκτρονικές επικοινωνίες και του Γενικού Κανονισμού Προστασίας Δεδομένων όσον αφορά τη διαχείριση cookies και συναφών τεχνολογιών.

Με σκοπό την πρακτική καθοδήγηση των υπευθύνων επεξεργασίας αλλά και την ενημέρωση των χρηστών των ελληνικών ιστοτόπων, η Αρχή εκδίδει κείμενο με ειδικές συστάσεις συμμόρφωσης στον συγκεκριμένο τομέα. Σε αυτό περιλαμβάνεται, υπό μορφή σημείων, καθοδήγηση για τη σύνομη χρήση τέτοιων τεχνολογιών καθώς και πρακτικές που πρέπει να αποφεύγονται.

Επισημαίνεται ότι η κωδικοποίηση των απαιτήσεων αυτών δεν συνιστά αλλαγή του ισχύοντος θεσμικού πλαισίου και της νομολογίας της Αρχής, προς τις προβλέψεις των οποίων οι υπεύθυνοι επεξεργασίας έχουν υποχρέωση συμμόρφωσης. Αναγνωρίζοντας όμως ότι μπορεί να απαιτηθεί κάποιος χρόνος προσαρμογής των μηχανισμών διαχείρισης που χρησιμοποιούνται από τις ιστοσελίδες, **η Αρχή καλεί όλους τους υπευθύνους επεξεργασίας να προσαρμοστούν εντός διμήνου το αργότερο.**

Σημεία συμμόρφωσης για υπευθύνους επεξεργασίας που διατηρούν διαδικτυακές ιστοσελίδες (sites)

Οι παρακάτω ρυθμίσεις εφαρμόζονται σε HTTP/S cookies, σε flash cookies, στον "τοπικό αποθηκευτικό χώρο" (local storage) που εφαρμόζεται στην HTML 5, σε αναγνώριση με τον υπολογισμό του ψηφιακού αποτυπώματος της τερματικής συσκευής, σε αναγνωριστικά που δημιουργούνται από τα λειτουργικά συστήματα (είτε προορίζονται για σκοπό διαφήμισης είτε όχι: IDFA, IDFV, Android ID κ.λπ.), σε αναγνωριστικά υλικού (διεύθυνση MAC, σειριακό αριθμό ή άλλο αναγνωριστικό συσκευής) κ.λπ.

Στο κείμενο που ακολουθεί χρησιμοποιείται ο όρος *ιχνηλάτης* ("tracker") ως ο πιο κατάλληλος να αποτυπώσει τις τεχνικές αυτές.

A. Υποχρέωση λήψης συγκατάθεσης και εξαιρέσεις

1. Για την τοποθέτηση ενός ιχνηλάτη σε τερματική συσκευή απαιτείται κατ' αρχήν η συγκατάθεση του χρήστη, ανεξάρτητα αν μέσω αυτού πραγματοποιείται τελικά επεξεργασία προσωπικών δεδομένων.
2. Οι ιχνηλάτες που εξαιρούνται από την υποχρέωση λήψης συγκατάθεσης είναι εκείνοι που θεωρούνται τεχνικά απαραίτητοι για την πραγματοποίηση της σύνδεσης στην ιστοσελίδα ή για την παροχή της υπηρεσίας διαδικτύου την οποία έχει ζητήσει ο ίδιος ο χρήστης.

Ενδεικτικές κατηγορίες ιχνηλατών (cookies και συναφών τεχνολογιών) που εμπίπτουν στην παραπάνω εξαίρεση είναι όσοι είναι απαραίτητοι:

- για την αναγνώριση ή/και διατήρηση περιεχομένου που εισάγει ο συνδρομητής ή χρήστης κατά τη διάρκεια μιας σύνδεσης (session) σε ιστοσελίδα καθ' όλη τη διάρκεια της συγκεκριμένης σύνδεσης, όπως το «καλάθι αγορών»
- για τη σύνδεση του συνδρομητή ή χρήστη σε υπηρεσίες που απαιτούν αυθεντικοποίηση
- για την ασφάλεια του χρήστη

- για την πραγματοποίηση της τεχνικής της κατανομής φορτίου (load balancing) σε μία σύνδεση σε ιστοσελίδα του διαδικτύου
 - για τη διατήρηση των επιλογών του χρήστη σχετικά με την παρουσίαση της ιστοσελίδας, π.χ. επιλογή γλώσσας, αποθήκευση ιστορικού αναζητήσεων
3. Οι ιχνηλάτες που εγκαθίστανται με σκοπό τη διαδικτυακή διαφήμιση (online advertizing) δεν εμπίπτουν στην εξαίρεση, επομένως επιτρέπονται μόνο εφόσον έχει ληφθεί προηγουμένως η συγκατάθεση του χρήστη κατόπιν κατάλληλης ενημέρωσης.
 4. Η χρήση ιχνηλατών τρίτων, όπως η υπηρεσία Google Analytics με σκοπό την στατιστική ανάλυση (web analytics), μπορεί να γίνει μόνο κατόπιν συγκατάθεσης του χρήστη της ιστοσελίδας.

Κακές πρακτικές

1. Γίνεται χρήση ιχνηλατών απαραίτητων για τη λειτουργία της ιστοσελίδας, αλλά δεν παρέχεται καμία ενημέρωση στο χρήστη.
2. Η χρήση Google Analytics με σκοπό τη στατιστική ανάλυση (web analytics) γίνεται μόνο με ενημέρωση στο χρήστη χωρίς να δίνεται η δυνατότητα απόρριψης ή χωρίς καν ενημέρωση.

B. Τρόπος και περιεχόμενο ενημέρωσης

1. Η ενημέρωση και η συγκατάθεση μπορεί να δίδονται μέσω της ιστοσελίδας του παρόχου υπηρεσίας του διαδικτύου με χρήση κατάλληλων μηχανισμών (π.χ. με αναδυόμενα παράθυρα (pop up) ή με ένα ενημερωτικό πλαίσιο (banner)).
2. Είναι θεμιτή η παροχή της ενημέρωσης μέσω πολλών επιπέδων, αρκεί να εξασφαλιστεί ότι η συγκατάθεση του χρήστη ζητείται αφού έχει ενημερωθεί ειδικά ο χρήστης, τουλάχιστον για τις κατηγορίες ιχνηλατών που χρησιμοποιούνται.

3. Μέσω του ενημερωτικού μηνύματος (είτε πρόκειται για αναδυόμενο παράθυρο είτε για άλλο τρόπο) πρέπει να παρέχεται ειδική ενημέρωση για το σκοπό του κάθε ιχνηλάτη που χρησιμοποιείται, και όχι γενική ενημέρωση για την χρήση ιχνηλατών.
4. Για κάθε ιχνηλάτη ή κατηγορία ιχνηλατών ιδίου σκοπού θα πρέπει να αναφέρονται η διάρκεια λειτουργίας, η ταυτότητα του υπευθύνου της επεξεργασίας, οι αποδέκτες ή οι κατηγορίες αποδεκτών των δεδομένων.
5. Το περιεχόμενο της ενημέρωσης θα πρέπει να είναι ευανάγνωστο ανεξαρτήτως της τερματικής συσκευής από όπου γίνεται η πρόσβαση (φορητή ή σταθερή συσκευή).

Κακές πρακτικές

1. Παρέχεται μόνο μια γενική ενημέρωση για τη χρήση ιχνηλατών μέσα σε ένα γενικό κείμενο πολιτικής προστασίας δεδομένων.
2. Η ενημέρωση για τη χρήση ιχνηλατών στο πρώτο επίπεδο του αναδυόμενου παραθύρου περιορίζεται μόνο σε γενικό κείμενο το οποίο αναφέρει ότι χρησιμοποιούνται τέτοιες τεχνικές, π.χ. cookies για την καλύτερη εμπειρία, καλύτερη παρουσίαση, κτλ.
3. Το κείμενο της ενημέρωσης δεν είναι ευανάγνωστο λόγω της μη προσαρμογής στο είδος της τερματικής συσκευής από όπου γίνεται η πρόσβαση (φορητή ή σταθερή συσκευή).

Γ. Τρόπος λήψης συγκατάθεσης

1. Η συγκατάθεση απαιτεί σαφή θετική ενέργεια. Προσυμπληρωμένα τετραγωνίδια, απλή συνέχιση πλοήγησης ή κύλιση οθόνης (scrolling) δεν είναι αποδεκτοί τρόποι παροχής συγκατάθεσης.

2. Δεν θεωρείται ότι υπάρχει συγκατάθεση του χρήστη στην περίπτωση κατά την οποία το πρόγραμμα πλοήγησης έχει ως επιλογή την αποδοχή των cookies.
3. Ελλείψει οποιασδήποτε εκδήλωσης επιλογής (ούτε αποδοχής ούτε απόρριψης), δεν πρέπει να γίνεται χρήση κανενός μη απαραίτητου ιχνηλάτη.
4. Θα πρέπει ο χρήστης να μπορεί, με τον ίδιο αριθμό ενεργειών («κλικ») και από το ίδιο επίπεδο, είτε να αποδέχεται τη χρήση των ιχνηλατών (εκείνων για τους οποίους απαιτείται συγκατάθεση) είτε να την απορρίπτει, είτε όλους είτε κάθε κατηγορία ξεχωριστά.
5. Ο χρήστης πρέπει να έχει τη δυνατότητα να ανακαλέσει τη συγκατάθεσή του με τον ίδιο τρόπο και με την ίδια ευκολία με τον οποίο τη δήλωσε.
6. Η μη παροχή συγκατάθεσης για τη χρήση ιχνηλατών δεν πρέπει να οδηγεί σε αποκλεισμό από την πρόσβαση στο περιεχόμενο της ιστοσελίδας (αποφυγή “cookie wall”).
7. Για να διασφαλιστεί ότι ο χρήστης δεν έχει επηρεαστεί από επιλογές σχεδιασμού υπέρ της επιλογής αποδοχής έναντι της επιλογής απόρριψης, συνιστάται η χρήση κουμπιών και γραμματοσειράς ίδιου μεγέθους, τονισμού και χρώματος, που να προσφέρει την ίδια ευκολία ανάγνωσης.
8. Ανεξαρτήτως αποδοχής ή απόρριψης των ιχνηλατών, η επανεμφάνιση του αναδυόμενου παραθύρου, ώστε να ερωτηθεί ξανά ο χρήστης, πρέπει να γίνεται μετά από τον ίδιο χρόνο. Δηλαδή, η διάρκεια «τήρησης» της επιλογής του χρήστη είναι η ίδια είτε ο χρήστης απορρίψει είτε αποδεχτεί τους ιχνηλάτες. Εξυπακούεται ότι η χρήση ιχνηλάτη για την αποθήκευση αυτής της επιλογής ενός χρήστη εντάσσεται στα τεχνικά απαραίτητα.

Κακές πρακτικές

1. Για τη λήψη συγκατάθεσης υπάρχει απλά μια επιλογή της μορφής «Εντάξει, ενημερώθηκα» ή «Εντάξει, συμφωνώ», χωρίς δυνατότητα να συνεχιστεί απρόσκοπτα η πλοήγηση (με απομάκρυνση του εν λόγω μηνύματος) αν ο χρήστης δεν επιλέξει το ανωτέρω.
2. Δεν υπάρχει η δυνατότητα απόρριψης της χρήσης ιχνηλατών στο αναδυόμενο παράθυρο, παρά μόνο αποδοχής όλων.
3. Η δυνατότητα απόρριψης της χρήσης ιχνηλατών δίνεται μόνο σε δεύτερο επίπεδο πληροφοριών, δηλαδή μετά το «κλικ» σε υπερσύνδεσμο με «περισσότερες πληροφορίες», «ρυθμίσεις».
4. Το κλείσιμο του αναδυόμενου παραθύρου/ενημερωτικού πλαισίου οδηγεί σε χρήση των μη απαραίτητων ιχνηλατών.
5. Η συνέχιση πλοήγησης ή το κύλισμα (scrolling) μετά την εμφάνιση του αναδυόμενου παραθύρου οδηγεί σε εγκατάσταση των μη απαραίτητων ιχνηλατών.
6. Το μέγεθος και το χρώμα του κουμπιού «αποδοχή» ή «συγκατάθεση» προδιαθέτει έντονα το χρήστη στην επιλογή του, π.χ. είναι πολύ μεγάλο και με έντονο χρώμα ή/και είναι προεπιλεγμένο.
7. Το αναδυόμενο παράθυρο δίνει μόνο τη δυνατότητα αποδοχής των μη απαραίτητων ιχνηλατών παραπέμποντας σε μια γενική πολιτική προστασίας δεδομένων ή απορρήτου.
8. Μετά την αποδοχή ή την απόρριψη από το χρήστη, δεν υπάρχει τρόπος αλλαγής των προτιμήσεών του.

9. Μετά την αποδοχή ή την απόρριψη από τον χρήστη, μπορεί να πραγματοποιηθεί αλλαγή των προτιμήσεών του μόνο μέσω αλλαγής ρυθμίσεων του φυλλομετρητή ιστού.

10. Στην περίπτωση απόρριψης των ιχνηλατών, ο χρήστης καλείται συνεχώς μέσω του αναδυόμενου παραθύρου να κάνει νέα επιλογή. Δεν ισχύει το ίδιο όταν αποδεχτεί, αφού η επιλογή του αυτή διατηρείται για μεγαλύτερο χρονικό διάστημα.