**Περίληψη της γνωμοδότησης του Ευρωπαίου Επόπτη Προστασίας Δεδομένων επί της κοινής ανακοίνωσης της Επιτροπής και της Ύπατης Εκπροσώπου της Ευρωπαϊκής Ένωσης για θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας σχετικά με τη «Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο: για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο» και επί της πρότασης οδηγίας της Επιτροπής σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση**

*(Το πλήρες κείμενο της παρούσας γνωμοδότησης διατίθεται στα αγγλικά, στα γαλλικά και στα γερμανικά μέσω του δικτυακού τόπου του ΕΕΠΔ στη διεύθυνση http://www.edps.europa.eu)*

(2014/C 32/10)

1. **Εισαγωγή**

1.1. *Διαβούλευση με τον ΕΕΠΔ*

1. Στις 7 Φεβρουαρίου 2013, η Επιτροπή και η Ύπατη Εκπρόσωπος της Ευρωπαϊκής Ένωσης για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας εξέδωσαν κοινή ανακοίνωση προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών σχετικά με τη «Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο: για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο» ([1]) (εφεξής «η κοινή ανακοίνωση», «η στρατηγική για την ασφάλεια στον κυβερνοχώρο» ή «η στρατηγική»).

2. Την ίδια ημερομηνία, η Επιτροπή εξέδωσε πρόταση οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών σε ολόκληρη την Ένωση ([2]) (εφεξής «η προτεινόμενη οδηγία» ή «η οδηγία»). Η πρόταση αυτή διαβιβάστηκε στις 7 Φεβρουαρίου 2013 στον ΕΕΠΔ για διαβούλευση.

3. Σε χρόνο προγενέστερο της έκδοσης της κοινής ανακοίνωσης και της πρότασης, δόθηκε στον ΕΕΠΔ η δυνατότητα να διαβιβάσει άτυπα σχόλια στην Επιτροπή. Ο ΕΕΠΔ εκφράζει την ικανοποίησή του για το γεγονός ότι ορισμένα από τα σχόλιά του ελήφθησαν υπόψη στην κοινή ανακοίνωση και στην πρόταση.

4. **Συμπεράσματα**

74. Ο ΕΕΠΔ εκφράζει την ικανοποίησή του για το γεγονός ότι η Επιτροπή και η Ύπατη Εκπρόσωπος της ΕΕ για Θέματα Εξωτερικής Πολιτικής και Πολιτικής Ασφάλειας έχουν προτείνει μια περιεκτική στρατηγική για την ασφάλεια στον κυβερνοχώρο, η οποία συμπληρώνεται με μια πρόταση οδηγίας σχετικά με μέτρα για την εξασφάλιση κοινού υψηλού επιπέδου ασφάλειας δικτύων και πληροφοριών (ΑΔΠ) στην ΕΕ. Η στρατηγική συμπληρώνει τις δράσεις πολιτικής που έχουν ήδη αναπτυχθεί από την ΕΕ στον τομέα της ασφάλειας δικτύων και πληροφοριών.

75. Ο ΕΕΠΔ επικροτεί το γεγονός ότι η στρατηγική υπερβαίνει το συμβατικό δίπολο ασφάλειας-προστασίας της ιδιωτικής ζωής, προβλέποντας τη ρητή αναγνώριση της προστασίας της ιδιωτικής ζωής και των δεδομένων ως θεμελιωδών αξιών επί των οποίων πρέπει να ερείδεται η πολιτική για την ασφάλεια στον κυβερνοχώρο της ΕΕ και παγκοσμίως. Ο ΕΕΠΔ επισημαίνει ότι η στρατηγική για την ασφάλεια στον κυβερνοχώρο και η προτεινόμενη οδηγία για την ΑΔΠ μπορούν να συμβάλλουν καθοριστικά στην προστασία του δικαιώματος προστασίας της ιδιωτικής ζωής και του δικαιώματος προστασίας των δεδομένων στο επιγραμμικό περιβάλλον. Παράλληλα όμως πρέπει να διασφαλίζεται ότι οι δύο αυτές πράξεις δεν συνεπάγονται τη λήψη μέτρων τα οποία θίγουν το δικαίωμα στην προστασία της ιδιωτικής ζωής και το δικαίωμα στην προστασία των δεδομένων.

76. Ο ΕΕΠΔ χαιρετίζει επίσης το γεγονός ότι η προστασία των δεδομένων αναφέρεται σε αρκετά σημεία της στρατηγικής και λαμβάνεται υπόψη στην προτεινόμενη οδηγία για την ΑΔΠ. Εντούτοις, εκφράζει τη δυσαρέσκειά του για το γεγονός ότι τόσο στη στρατηγική όσο και στην προτεινόμενη οδηγία η συμβολή της ισχύουσας και της επικείμενης νομοθεσίας για την προστασία των δεδομένων στην ασφάλεια δεν αναδεικνύεται ικανοποιητικά και δεν διασφαλίζεται πλήρως η συμπληρωματικότητα των υποχρεώσεων που απορρέουν από την προτεινόμενη οδηγία ή άλλων στοιχείων της στρατηγικής προς τις υποχρεώσεις για την προστασία των δεδομένων, ούτε λαμβάνεται επαρκής μέριμνα για την αποφυγή αλληλοεπικαλύψεων ή αντιφάσεων μεταξύ τους.

77. Επιπλέον, ο ΕΕΠΔ επισημαίνει ότι λόγω της πλημμελούς συνεκτίμησης άλλων παράλληλων πρωτοβουλιών της Επιτροπής και εν εξελίξει νομοθετικών διαδικασιών, όπως η μεταρρύθμιση της προστασίας των δεδομένων και η πρόταση κανονισμού για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης, η στρατηγική για την ασφάλεια στον κυβερνοχώρο δεν καταφέρνει να προκρίνει μια πραγματικά περιεκτική και ολιστική οπτική της

([1]) JOIN(2013) 1 τελικό.
([2]) COM(2013) 48 τελικό.

ασφάλειας στον κυβερνοχώρο της ΕΕ, με κίνδυνο κάτι τέτοιο να διαιωνίσει μια αποσπασματική και κατακερματισμένη προσέγγιση. Ο ΕΕΠΔ επισημαίνει ομοίως την αδυναμία της προτεινόμενης οδηγίας για την ΑΔΠ να διαμορφώσει μια ολοκληρωμένη προσέγγιση της ασφάλειας στην ΕΕ, φρονώντας ότι η πληρέστερη υποχρέωση προστασίας δικτύων και ασφάλειας που περιέχεται στο δίκαιο της ΕΕ διατυπώνεται στη νομοθεσία για την προστασία των δεδομένων.

78. Ο ΕΕΠΔ αποδοκιμάζει επίσης την πλημμελή συνεκτίμηση του σημαντικού ρόλου των αρχών προστασίας των δεδομένων στην εφαρμογή και στην επιβολή των υποχρεώσεων ασφάλειας και στη βελτίωση της ασφάλειας στον κυβερνοχώρο.

79. Όσον αφορά τη στρατηγική για την ασφάλεια στον κυβερνοχώρο, ο ΕΕΠΔ υπογραμμίζει ότι:

— Ο σαφής ορισμός των όρων «ανθεκτικότητα όσον αφορά την ασφάλεια στον κυβερνοχώρο», «έγκλημα στον κυβερνοχώρο» και «άμυνα στον κυβερνοχώρο» είναι ιδιαίτερα σημαντικός, δεδομένου ότι οι όροι αυτοί χρησιμοποιούνται για να αιτιολογήσουν τη λήψη ειδικών μέτρων τα οποία μπορούν να θίξουν τα θεμελιώδη δικαιώματα, περιλαμβανομένου του δικαιώματος προστασίας της ιδιωτικής ζωής και του δικαιώματος προστασίας των δεδομένων. Παρόλα αυτά, οι ορισμοί του «εγκλήματος στον κυβερνοχώρο» που διατυπώνονται στη στρατηγική και στη σύμβαση για το έγκλημα στον κυβερνοχώρο παραμένουν αρκετά ευρείς. Κρίνεται συνεπώς προτιμητέος ο *συσταλτικός* έναντι του διασταλτικού ορισμού του «εγκλήματος στον κυβερνοχώρο».

— Η νομοθεσία για την προστασία των δεδομένων πρέπει να εφαρμόζεται σε κάθε μέτρο της στρατηγικής το οποίο συνεπάγεται την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Μολονότι στα τμήματα που αφορούν το έγκλημα και την άμυνα στον κυβερνοχώρο δεν γίνεται ρητή μνεία στη νομοθεσία για την προστασία των δεδομένων, ο ΕΕΠΔ επισημαίνει ότι πολλά από τα μέτρα που προβλέπεται να υλοποιηθούν στους συγκεκριμένους τομείς συνεπάγονται την επεξεργασία δεδομένων προσωπικού χαρακτήρα και, κατά συνέπεια, εμπίπτουν στο πεδίο εφαρμογής της ισχύουσας νομοθεσίας για την προστασία δεδομένων. Ο ΕΕΠΔ σημειώνει επίσης ότι πολλά μέτρα συνίστανται στη θέσπιση μηχανισμών συντονισμού στο πλαίσιο των οποίων οι διαδικασίες ανταλλαγής δεδομένων προϋποθέτουν την εφαρμογή κατάλληλων εγγυήσεων για την προστασία των δεδομένων.

— Οι αρχές προστασίας των δεδομένων διαδραματίζουν σημαντικό ρόλο στο πλαίσιο της ασφάλειας στον κυβερνοχώρο. Ως θεματοφύλακες των δικαιωμάτων των προσώπων στην προστασία της προσωπικής τους ζωής και των δεδομένων που τα αφορούν, οι αρχές προστασίας των δεδομένων μεριμνούν ενεργά για την προστασία των δεδομένων προσωπικού χαρακτήρα εντός και εκτός γραμμής. Κατά συνέπεια, πρέπει να αναλαμβάνουν ως εποπτικοί φορείς τον δέοντα ρόλο στην εφαρμογή μέτρων που συνεπάγονται την επεξεργασία δεδομένων προσωπικού χαρακτήρα (όπως η έναρξη του πιλοτικού έργου της ΕΕ για την καταπολέμηση των δικτύων ρομπότ (botnet) και του κακόβουλου λογισμικού). Κατά την εκτέλεση των καθηκόντων τους, όπως η ανταλλαγή βέλτιστων πρακτικών και η υλοποίηση μέτρων ευαισθητοποίησης, οι εποπτικές αρχές πρέπει να λαμβάνουν τη συνδρομή άλλων παραγόντων στον τομέα της ασφάλειας στον κυβερνοχώρο. Ο ΕΕΠΔ και οι εθνικές αρχές προστασίας των δεδομένων πρέπει να συμμετάσχουν με πρόσφορο τρόπο στη διάσκεψη υψηλού επιπέδου που θα διεξαχθεί το 2014 για την αξιολόγηση της προόδου ως προς την εφαρμογή της στρατηγικής.

80. Όσον αφορά την πρόταση οδηγίας για την ΑΔΠ, ο ΕΕΠΔ συνιστά στους νομοθέτες:

— να αποσαφηνίσουν με μεγαλύτερη βεβαιότητα στο άρθρο 3 παράγραφος 8 τον ορισμό των φορέων της αγοράς που εμπίπτουν στο πεδίο εφαρμογής της πρότασης και να καταρτίσουν έναν διεξοδικό κατάλογο όλων των ενδιαφερόμενων μερών, προκειμένου να διασφαλίσουν της εφαρμογή μιας πλήρως εναρμονισμένης και ολοκληρωμένης προσέγγισης της ασφάλειας σε επίπεδο ΕΕ

— να διευκρινίσουν στο άρθρο 1 παράγραφος 2 στοιχείο γ) ότι η προτεινόμενη οδηγία εφαρμόζεται και για τα θεσμικά όργανα και τους οργανισμούς της ΕΕ και να συμπεριλάβουν στο άρθρο 1 παράγραφος 5 της πρότασης παραπομπή στον κανονισμό (ΕΚ) αριθ. 45/2001

— να προσδώσουν έναν πιο οριζόντιο χαρακτήρα στην παρούσα πρόταση σε ό,τι αφορά την ασφάλεια, συμπεριλαμβάνοντας στο άρθρο 1 τη ρητή επιφύλαξη υφιστάμενων ή μελλοντικών πιο αναλυτικών κανόνων σε συγκεκριμένους τομείς (όπως οι κανόνες που πρόκειται να θεσπιστούν σχετικά με τους παρόχους υπηρεσιών εμπιστοσύνης στον προτεινόμενο κανονισμό σχετικά με την ηλεκτρονική ταυτοποίηση)

— να προσθέσουν αιτιολογική σκέψη η οποία θα επεξηγεί την ανάγκη ενσωμάτωσης της αρχής της προστασίας των δεδομένων ήδη από τα πρώιμα στάδια του σχεδιασμού των μηχανισμών που θεσπίζονται στην πρόταση και καθόλη τη διάρκεια του κύκλου ζωής των σχετικών διεργασιών, διαδικασιών, οργανωτικών δομών, τεχνικών και υποδομών, λαμβανομένου υπόψη του κανονισμού για την προστασία των δεδομένων

— να αποσαφηνίσουν τους ορισμούς του «συστήματος δικτύων και πληροφοριών» στο άρθρο 3 παράγραφος 1 και του «συμβάντος» στο άρθρο 3 παράγραφος 4, και να αντικαταστήσουν στο άρθρο 5 παράγραφος 2 την υποχρέωση κατάρτισης ενός «σχεδίου εκτίμησης του κινδύνου» με τη «δημιουργία και διατήρηση ενός πλαισίου διαχείρισης του κινδύνου»

— να διευκρινίσουν στο άρθρο 1 παράγραφος 6 ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα δικαιολογείται βάσει του άρθρου 7 στοιχείο ε) της οδηγίας 95/46/ΕΚ στον βαθμό που είναι αναγκαία για την επίτευξη των στόχων δημοσίου συμφέροντος που επιδιώκει η προτεινόμενη οδηγία. Πρέπει, ωστόσο, να διασφαλίζεται η δέουσα τήρηση των αρχών της αναγκαιότητας και την αναλογικότητας, ούτως ώστε να υποβάλλονται σε επεξεργασία μόνο τα δεδομένα που είναι άκρως αναγκαία για την επίτευξη του επιδιωκόμενου σκοπού

— να καθορίσουν στο άρθρο 14 τις συνθήκες υπό τις οποίες απαιτείται κοινοποίηση, το περιεχόμενο και τη μορφή αυτής, περιλαμβανομένων των τύπων των δεδομένων προσωπικού χαρακτήρα που πρέπει να κοινοποιούνται, καθώς και το κατά πόσον — και σε ποιον βαθμό — η κοινοποίηση και τα σχετικά δικαιολογητικά θα συμπεριλαμβάνουν λεπτομέρειες σχετικά με τα δεδομένα προσωπικού χαρακτήρα που επηρεάζονται από κάποιο συγκεκριμένο συμβάν ασφάλειας (περιλαμβανομένων των διευθύνσεων IP). Πρέπει να λαμβάνεται υπόψη το γεγονός ότι η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες για την ΑΔΠ αρχές στο πλαίσιο ενός συμβάντος ασφάλειας πρέπει να επιτρέπεται μόνο εφόσον οι πράξεις αυτές είναι απολύτως αναγκαίες. Στην πρόταση πρέπει επίσης να καθορίζονται κατάλληλες εγγυήσεις για τη διασφάλιση της επαρκούς προστασίας των δεδομένων που επεξεργάζονται οι αρμόδιες για την ΑΔΠ αρχές

— να αποσαφηνίσουν στο άρθρο 14 ότι οι κοινοποιήσεις συμβάντων δυνάμει του άρθρου 14 παράγραφος 2 πρέπει να πραγματοποιούνται με την επιφύλαξη των υποχρεώσεων κοινοποίησης παραβιάσεων των δεδομένων προσωπικού χαρακτήρα σύμφωνα με την ισχύουσα νομοθεσία για την προστασία δεδομένων. Στην πρόταση πρέπει να θεσπίζονται οι βασικές πτυχές της διαδικασίας σύμπραξης των αρμόδιων για την ΑΔΠ αρχών με τις αρχές προστασίας των δεδομένων σε περιπτώσεις συμβάντων ασφάλειας κατά τις οποίες παραβιάζονται δεδομένα προσωπικού χαρακτήρα

— να τροποποιήσουν το άρθρο 14 παράγραφος 8 κατά τρόπο ώστε η εξαίρεση των πολύ μικρών επιχειρήσεων από το πεδίο κοινοποίησης να μην ισχύει για τους φορείς που διαδραματίζουν κρίσιμο ρόλο στην παροχή υπηρεσιών κοινωνίας της πληροφορίας, για παράδειγμα ανάλογα με τη φύση των πληροφοριών που επεξεργάζονται (π.χ. βιομετρικά ή ευαίσθητα δεδομένα)

— να προσθέσουν στην πρόταση διατάξεις σχετικά με την περαιτέρω ανταλλαγή δεδομένων προσωπικού χαρακτήρα μεταξύ των αρμόδιων για την ΑΔΠ αρχών και άλλων αποδεκτών κατά τρόπο ώστε να διασφαλίζεται i) ότι τα δεδομένα προσωπικού χαρακτήρα κοινοποιούνται μόνο σε αποδέκτες οι οποίοι προβαίνουν σε πράξεις επεξεργασίας που είναι αναγκαίες για την εκτέλεση των καθηκόντων τους σύμφωνα με κάποια κατάλληλη νομική βάση και ii) ότι οι πληροφορίες αυτές περιορίζονται σε όσες είναι άκρως αναγκαίες για την εκτέλεση των καθηκόντων τους. Πρέπει επίσης να εξετάζονται τα μέτρα στα οποία προβαίνουν οι οντότητες που παρέχουν δεδομένα στο δίκτυο ανταλλαγής πληροφοριών ώστε να διασφαλίζεται η τήρηση της αρχής του περιορισμού του σκοπού

— να προσδιορίσουν το χρονικό όριο διατήρησης των δεδομένων προσωπικού χαρακτήρα για τους σκοπούς που καθορίζονται στην προτεινόμενη οδηγία, ιδίως σε ό,τι αφορά τη διατήρηση δεδομένων είτε από τις αρμόδιες για την ΑΔΠ αρχές είτε εντός της ασφαλούς υποδομής του δικτύου συνεργασίας

— να υπενθυμίσουν στις αρμόδιες για την ΑΔΠ αρχές την υποχρέωσή τους να παρέχουν κατάλληλες πληροφορίες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα στα πρόσωπα στα οποία αναφέρονται τα δεδομένα, αναρτώντας για παράδειγμα στον δικτυακό τους τόπο την οικεία πολιτική για την προστασία της ιδιωτικής ζωής

— να προσθέσουν διάταξη σχετικά με το επίπεδο ασφάλειας που πρέπει να τηρούν οι αρμόδιες για την ΑΔΠ αρχές όσον αφορά τις πληροφορίες που συλλέγονται, υποβάλλονται σε επεξεργασία και ανταλλάσσονται. Όσον αφορά την προστασία δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες για την ΑΔΠ αρχές, πρέπει να προστεθεί παραπομπή στις απαιτήσεις που περιέχονται σχετικά με την ασφάλεια στο άρθρο 17 της οδηγίας 95/46/ΕΚ

— να αποσαφηνίσουν στο άρθρο 9 παράγραφος 2 ότι τα κριτήρια για την συμμετοχή των κρατών μελών στο ασφαλές σύστημα ανταλλαγής πληροφοριών πρέπει να διασφαλίζουν ότι όλοι οι συμμετέχοντες στο εν λόγω σύστημα εγγυώνται ανά πάσα στιγμή κατά τη διάρκεια της επεξεργασίας την τήρηση υψηλού επιπέδου ασφάλειας και ανθεκτικότητας. Τα κριτήρια αυτά πρέπει να περιλαμβάνουν κατάλληλα μέτρα για την τήρηση απορρήτου και την ασφάλεια σύμφωνα με τα άρθρα 16 και 17 της οδηγίας 95/46/ΕΚ και τα άρθρα 21 και 22 του κανονισμού (ΕΚ) αριθ. 45/2001. Κατά τη συμμετοχή της στο ασφαλές σύστημα ανταλλαγής πληροφοριών με την ιδιότητα του υπευθύνου επεξεργασίας, η Επιτροπή πρέπει να δεσμεύεται ρητώς από αυτά τα κριτήρια

— να προσθέσουν στο άρθρο 9 περιγραφή των ρόλων και των αρμοδιοτήτων της Επιτροπής και των κρατών μελών στη δημιουργία, στη λειτουργία και στη συντήρηση του ασφαλούς συστήματος ανταλλαγής πληροφοριών και να μεριμνήσουν για τον σχεδιασμό του συστήματος σύμφωνα με τις αρχές της προστασίας δεδομένων ήδη από τον σχεδιασμό και εξορισμού και της ασφάλειας ήδη από τον σχεδιασμό, και

— να προσθέσουν στο άρθρο 13 την υποχρέωση διαβίβασης δεδομένων προσωπικού χαρακτήρα σε αποδέκτες εκτός της ΕΕ σύμφωνα με τα άρθρα 25 και 26 της οδηγίας 95/46/ΕΚ και το άρθρο 9 του κανονισμού (ΕΚ) αριθ. 45/2001.

Βρυξέλλες, 14 Ιουνίου 2013.

Peter HUSTINX

*Ευρωπαίος Επόπτης Προστασίας Δεδομένων*