ΚΑΝΟΝΙΣΜΟΙ

ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) αριθ. 611/2013 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 24ης Ιουνίου 2013

σχετικά με τα εφαρμοστέα μέτρα για την κοινοποίηση παραβιάσεων προσωπικών δεδομένων βάσει της οδηγίας 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη την οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες) ([1]), και ιδίως το άρθρο 4 παράγραφος 5,

Έπειτα από διαβούλευση με τον ευρωπαϊκό οργανισμό για την ασφάλεια δικτύων και πληροφοριών (ENISA),

Έπειτα από διαβούλευση με την ομάδα εργασίας σχετικά με την προστασία των προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η οποία έχει συσταθεί δυνάμει του άρθρου 29 της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών ([2]) (ομάδα εργασίας του άρθρου 29),

Έπειτα από διαβούλευση με τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων ((EDPS),

Εκτιμώντας τα ακόλουθα:

(1) Η οδηγία 2002/58/ΕΚ προβλέπει την εναρμόνιση των εθνικών διατάξεων οι οποίες απαιτούνται προκειμένου να διασφαλίζεται ισοδύναμο επίπεδο προστασίας των θεμελιωδών δικαιωμάτων και ελευθεριών, και ιδίως του δικαιώματος στην ιδιωτική ζωή και την εμπιστευτικότητα, όσον αφορά την επεξεργασία προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, καθώς και να διασφαλίζεται η ελεύθερη κυκλοφορία των δεδομένων αυτών, καθώς και του εξοπλισμού και των υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ένωση.

(2) Βάσει του άρθρου 4 της οδηγίας 2002/58/ΕΚ, οι φορείς παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών υποχρεούται να κοινοποιούν στις αρμόδιες εθνικές αρχές, καθώς και —σε ορισμένες περιπτώσεις— στους ενδιαφερόμενους συνδρομητές και άτομα, τις παραβιάσεις προσωπικών δεδομένων. Η παραβίαση προσωπικών δεδομένων ορίζεται στο άρθρο 2 στοιχείο θ) της οδηγίας 2002/58/ΕΚ ως παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινολόγηση ή πρόσβαση σε προσωπικά δεδομένα που έχουν διαβιβαστεί, αποθηκευτεί ή κατ' άλλο τρόπο υποβληθεί σε επεξεργασία, σε συνδυασμό με την παροχή διαθέσιμων στο κοινό ηλεκτρονικών υπηρεσιών επικοινωνιών στην Ένωση.

(3) Προκειμένου να διασφαλιστεί η συνοχή κατά την εφαρμογή των μέτρων που αναφέρονται στις παραγράφους 2, 3 και 4 του άρθρου 4 της οδηγίας 2002/58/ΕΚ, με το άρθρο 4 παράγραφος 5 εξουσιοδοτείται η Επιτροπή να λαμβάνει τεχνικά εκτελεστικά μέτρα όσον αφορά τις συνθήκες, το μορφότυπο και τις διαδικασίες που εφαρμόζονται στις απαιτήσεις πληροφόρησης και κοινοποίησης που αναφέρονται στο εν λόγω άρθρο.

(4) Ή Η ύπαρξη διαφορετικών εθνικών απαιτήσεων ενδέχεται εν προκειμένω να οδηγήσει σε νομική αβεβαιότητα, συνθετότερες και επαχθέστερες διαδικασίες, καθώς και να συνεπάγεται σημαντικό διοικητικό κόστος για παρόχους που λειτουργούν διασυνοριακά. Κατά συνέπεια, η Επιτροπή κρίνει απαραίτητη τη θέσπιση σχετικών τεχνικών εκτελεστικών μέτρων.

(5) Ο παρών κανονισμός περιορίζεται στην κοινοποίηση περιπτώσεων παραβίασης προσωπικών δεδομένων και επομένως δεν ορίζει τεχνικά εκτελεστικά μέτρα όσον αφορά το άρθρο 4 παράγραφος 2 της οδηγίας 2002/58/ΕΚ για ενημέρωση των συνδρομητών σε περίπτωση συγκεκριμένου κινδύνου παραβίασης της ασφάλειας του δικτύου.

(6) Από το πρώτο εδάφιο του άρθρου 4 παράγραφος 3 της οδηγίας 2002/58/ΕΚ συνάγεται ότι οι πάροχοι οφείλουν να κοινοποιούν στην αρμόδια εθνική αρχή κάθε παραβίαση προσωπικών δεδομένων. Επομένως, ο πάροχος δεν πρέπει να διαθέτει την ευχέρεια να αποφασίζει αν θα κοινοποιεί ή όχι στην αρμόδια εθνική αρχή. Ωστόσο, αυτό δεν πρέπει να εμποδίζει την αρμόδια εθνική αρχή να παραχωρεί προτεραιότητα στη διερεύνηση ορισμένων παραβάσεων κατά τον τρόπο που αυτή κρίνει αναγκαίο, σύμφωνα με την ισχύουσα νομοθεσία, ούτε και να λάβει τα αναγκαία μέτρα για να αποφύγει την υπερβολική ή την ελλιπή αναφορά παραβιάσεων προσωπικών δεδομένων.

(7) Είναι σκόπιμο να προβλεφθεί ένα σύστημα για την κοινοποίηση στην αρμόδια εθνική αρχή παραβιάσεων προσωπικών δεδομένων, που θα αποτελείται, εφόσον πληρούνται ορισμένες προϋποθέσεις, από διάφορες φάσεις, καθεμία από τις οποίες υπάγεται σε ορισμένα χρονικά όρια. Το σύστημα αυτό έχει ως στόχο να εξασφαλίσει ότι η αρμόδια εθνική αρχή ενημερώνεται το συντομότερο και όσο το δυνατόν πληρέστερα, χωρίς όμως αδικαιολόγητη παρακώλυση του παρόχου στις προσπάθειές του να διερευνήσει την παραβίαση και να λάβει τα αναγκαία μέτρα για περιορισμό και αντιμετώπιση των συνεπειών της.

([1]) ΕΕ L 201 της 31.7.2002, σ. 37.
([2]) ΕΕ L 281 της 23.11.1995, σ. 31.

(8) Ούτε απλή υποψία ότι έχει συμβεί παραβίαση προσωπικών δεδομένων, ούτε απλή ανίχνευση ενός συμβάντος χωρίς να είναι διαθέσιμες επαρκείς πληροφορίες, παρά τις φιλότιμες προσπάθειες του παρόχου προς τούτο, αρκούν για να θεωρηθεί ότι έχει διαπιστωθεί παραβίαση προσωπικών δεδομένων κατά τους σκοπούς του παρόντος κανονισμού. Ιδιαίτερη προσοχή πρέπει να δοθεί εν προκειμένω στη διαθεσιμότητα των πληροφοριών που αναφέρονται στο παράρτημα Ι.

(9) Στο πλαίσιο της εφαρμογής του παρόντος κανονισμού, οι αρμόδιες εθνικές αρχές πρέπει να συνεργάζονται σε περιπτώσεις παραβιάσεων προσωπικών δεδομένων με διασυνοριακή διάσταση.

(10) Ο παρών κανονισμός δεν προβλέπει πρόσθετες προδιαγραφές για την απογραφή των παραβιάσεων προσωπικών δεδομένων που οφείλουν να διατηρούν οι πάροχοι, δεδομένου ότι στο άρθρο 4 της οδηγίας 2002/58/ΕΚ ορίζεται εξαντλητικά το περιεχόμενό της. Ωστόσο, οι πάροχοι μπορούν να παραπέμπουν στον παρόντα κανονισμό για τον καθορισμό της μορφής της απογραφής.

(11) Όλες οι αρμόδιες εθνικές αρχές οφείλουν να διαθέτουν ένα ασφαλές ηλεκτρονικό μέσο ώστε οι πάροχοι να κοινοποιούν παραβιάσεις προσωπικών δεδομένων σε κοινό μορφότυπο, με βάση ένα πρότυπο όπως το XML, το οποίο περιέχει τις πληροφορίες που καθορίζονται στο παράρτημα Ι στις αντίστοιχες γλώσσες, έτσι ώστε να μπορούν όλοι οι πάροχοι εντός της Ένωσης να ακολουθούν παρόμοια διαδικασία κοινοποίησης, ανεξάρτητα από το πού βρίσκονται ή πού συνέβη η παραβίαση προσωπικών δεδομένων. Στο πλαίσιο αυτό, η Επιτροπή πρέπει να διευκολύνει την εφαρμογή των ασφαλών ηλεκτρονικών μέσων οργανώνοντας συναντήσεις με τις αρμόδιες εθνικές αρχές, όπου είναι αναγκαίο.

(12) Κατά την εκτίμηση αν μια παραβίαση προσωπικών δεδομένων είναι πιθανό να επηρεάσει αρνητικά τα προσωπικά δεδομένα ή την ιδιωτική ζωή ενός συνδρομητή ή ατόμου, πρέπει να λαμβάνονται ιδίως υπόψη ο χαρακτήρας και το περιεχόμενο των εν λόγω δεδομένων προσωπικού χαρακτήρα, ιδίως όταν τα δεδομένα αφορούν οικονομικές πληροφορίες, όπως στοιχεία πιστωτικών καρτών και στοιχεία τραπεζικών λογαριασμών· ειδικές κατηγορίες δεδομένων που αναφέρονται στο άρθρο 8 παράγραφος 1 της οδηγίας 95/46/ΕΚ· και ορισμένα στοιχεία που σχετίζονται ειδικότερα με την παροχή υπηρεσιών τηλεφωνίας ή διαδικτύου, δηλαδή δεδομένα ηλε-ταχυδρομείου, γεωγραφικής θέσης, διαδικτυακά αρχεία καταγραφής, ιστορικά ιστοπεριήγησης και αναλυτικούς καταλόγους κλήσεων.

(13) Σε εξαιρετικές περιπτώσεις, πρέπει να επιτρέπεται στον πάροχο να καθυστερήσει για εύλογο χρονικό διάστημα την κοινοποίηση στον συνδρομητή ή άτομο, εφόσον η γνωστοποίηση στον συνδρομητή ή άτομο ενδέχεται να θέσει σε κίνδυνο την ορθή διερεύνηση της παραβίασης προσωπικών δεδομένων. Στο πλαίσιο αυτό, στις εξαιρετικές περιστάσεις μπορεί να περιλαμβάνεται διερεύνηση ποινικών υποθέσεων, καθώς και άλλες παραβιάσεις προσωπικών δεδομένων που δεν ισοδυναμούν με σοβαρό έγκλημα, αλλά για τις οποίες μπορεί να είναι σκόπιμη η αναβολή της κοινοποίησης Σε κάθε περίπτωση, πρέπει να εναπόκειται στην αρμόδια εθνική αρχή να αξιολογήσει, κατά περίπτωση και υπό το φως των περιστάσεων, εάν συμφωνήσει στην αναβολή ή αν απαιτήσει κοινοποίηση.

(14) Μολονότι οι πάροχοι πρέπει να διαθέτουν τα στοιχεία επικοινωνίας των συνδρομητών τους, δεδομένης της άμεσης συμβατικής σχέσης τους, οι πληροφορίες αυτές ενδέχεται να μην υπάρχουν για άλλα άτομα που θίγονται από την παραβίαση προσωπικών δεδομένων. Σε τέτοια περίπτωση, πρέπει να επιτρέπεται στον πάροχο να ενημερώσει αρχικά τα άτομα αυτά μέσω διαφημίσεων σε μεγάλα εθνικά ή περιφερειακά μέσα επικοινωνίας, όπως είναι οι εφημερίδες, και το συντομότερο δυνατό να ακολουθεί ατομική κοινοποίηση, όπως προβλέπεται στον παρόντα κανονισμό. Επομένως, ο πάροχος δεν υποχρεούται αφεαυτού να ενημερώσει μέσω των μέσων επικοινωνίας, αλλά έχει εντολή να ενεργεί κατ' αυτόν τον τρόπο, εφόσον επιθυμεί, όταν πρόκειται ακόμα για τη διαδικασία εντοπισμού όλων των ατόμων που επηρεάζονται.

(15) Οι πληροφορίες σχετικά με την παράβαση πρέπει να χρησιμοποιούνται αποκλειστικά για την παράβαση και να μην σχετίζονται με πληροφορίες σχετικά με άλλο θέμα. Για παράδειγμα, η συμπερίληψη πληροφοριών σχετικά με παραβίαση προσωπικών δεδομένων σε ένα κανονικό τιμολόγιο δεν πρέπει να θεωρείται επαρκές μέσο για να γνωστοποιηθεί μια παραβίαση προσωπικών δεδομένων.

(16) Ο παρών κανονισμός δεν καθορίζει συγκεκριμένα τεχνολογικά μέτρα προστασίας που να δικαιολογούν παρέκκλιση από την υποχρέωση κοινοποίησης παραβιάσεων προσωπικών δεδομένων σε συνδρομητές ή άτομα, καθώς τα μέτρα αυτά ενδέχεται να αλλάξουν με την πάροδο του χρόνου, ανάλογα με τις τεχνολογικές εξελίξεις. Η Επιτροπή πρέπει, ωστόσο, να είναι σε θέση να δημοσιεύσει ενδεικτικό κατάλογο τέτοιων συγκεκριμένων τεχνολογικών μέτρων προστασίας σύμφωνα με τρέχουσες πρακτικές.

(17) Η εφαρμογή κρυπτοθέτησης ή κατακερματισμού δεν πρέπει να θεωρείται αφεαυτής επαρκής ώστε να επιτρέψει στους παρόχους να υποστηρίζουν γενικά ότι έχουν εκπληρώσει τη γενική υποχρέωση ασφάλειας που καθορίζεται στο άρθρο 17 της οδηγίας 95/46/ΕΚ. Σε αυτό το πλαίσιο, οι πάροχοι οφείλουν επίσης να εφαρμόζουν επαρκή οργανωτικά και τεχνικά μέτρα για την πρόληψη, τον εντοπισμό και τον αποκλεισμό των παραβιάσεων προσωπικών δεδομένων. Οι πάροχοι πρέπει να εξετάζουν κάθε υπολειπόμενο κίνδυνο που ενδεχομένως υπάρχει μετά την εκτέλεση των ελέγχων ώστε να αντιληφθούν πού είναι πιθανό να παρουσιαστούν παραβιάσεις προσωπικών δεδομένων.

(18) Σε περίπτωση που ο πάροχος χρησιμοποιεί άλλο πάροχο για την εκτέλεση μέρους της υπηρεσίας, για παράδειγμα σε σχέση με την τιμολόγηση ή τη διαχείριση λειτουργιών, ο

εν λόγω άλλος πάροχος που δεν έχει άμεση συμβατική σχέση με τον τελικό χρήστη δεν υποχρεούται να εκδίδει κοινοποιήσεις σε περίπτωση παραβίασης προσωπικών δεδομένων. Αντ' αυτού, πρέπει να ειδοποιήσουν και να ενημερώσουν τον πάροχο με τον οποίο έχουν άμεση συμβατική σχέση. Αυτό πρέπει να ισχύει και στο πλαίσιο της χονδρικής παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών, όταν τυπικά ο πάροχος χονδρικής δεν έχει άμεση συμβατική σχέση με τον τελικό χρήστη.

(19) Η οδηγία 95/46/ΕΚ καθορίζει το γενικό πλαίσιο για την προστασία των προσωπικών δεδομένων στην Ευρωπαϊκή Ένωση. Η Επιτροπή υπέβαλε πρόταση κανονισμού του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την αντικατάσταση της οδηγίας 95/46/ΕΚ (κανονισμός για την προστασία των δεδομένων). Ο προτεινόμενος κανονισμός για την προστασία των δεδομένων θα εισήγαγε υποχρέωση για όλους τους υπευθύνους επεξεργασίας δεδομένων να κοινοποιούν παραβιάσεις προσωπικών δεδομένων, με βάση το άρθρο 4 παράγραφος 3 της οδηγίας 2002/58/ΕΚ. Ο παρών κανονισμός της Επιτροπής είναι απόλυτα συνεπής με αυτό το προτεινόμενο μέτρο.

(20) Ο προτεινόμενος κανονισμός για την προστασία των δεδομένων προχωρεί επίσης σε περιορισμένο αριθμό τεχνικών προσαρμογών στην οδηγία 2002/58/ΕΚ, ώστε να ληφθεί υπόψη η μετατροπή της οδηγίας 95/46/ΕΚ σε κανονισμό. Οι ουσιαστικές έννομες συνέπειες του νέου κανονισμού για την οδηγία 2002/58/ΕΚ, θα αποτελέσουν αντικείμενο επανεξέτασης από την Επιτροπή.

(21) Η εφαρμογή του παρόντος κανονισμού πρέπει να αναθεωρηθεί τρία έτη μετά την έναρξη ισχύος του, ενώ το περιεχόμενο του πρέπει να επανεξεταστεί υπό το πρίσμα του νομικού πλαισίου που θα ισχύει την εποχή εκείνη, συμπεριλαμβανομένου του προτεινόμενου κανονισμού για την προστασία των δεδομένων. Η αναθεώρηση του παρόντος κανονισμού πρέπει να συνδέεται, όπου είναι δυνατόν σε οποιαδήποτε μελλοντική αναθεώρηση της οδηγίας 2002/58/ΕΚ.

(22) Η εφαρμογή του παρόντος κανονισμού μπορεί να αξιολογηθεί με βάση, μεταξύ άλλων, τυχόν στατιστικές που τηρούν οι αρμόδιες εθνικές αρχές σχετικά με παραβιάσεις προσωπικών δεδομένων οι οποίες τους έχουν κοινοποιηθεί. Αυτά τα στατιστικά στοιχεία μπορεί να περιλαμβάνουν, για παράδειγμα, πληροφορίες σχετικά με τον αριθμό των παραβιάσεων προσωπικών δεδομένων που έχουν κοινοποιηθεί στην αρμόδια εθνική αρχή, τον αριθμό των παραβιάσεων προσωπικών δεδομένων που έχουν κοινοποιηθεί στον συνδρομητή ή άτομο, το χρόνο που απαιτήθηκε για την επίλυση της παραβίασης προσωπικών δεδομένων, καθώς και αν ελήφθησαν τεχνολογικά μέτρα προστασίας. Οι στατιστικές αυτές πρέπει να παρέχουν στην Επιτροπή και τα κράτη μέλη συνεπή και συγκρίσιμα στατιστικά στοιχεία, ενώ δεν πρέπει να αποκαλύπτονται ούτε η ταυτότητα του κοινοποιούντος παρόχου, ούτε των εμπλεκόμενων συνδρομητών ή ατόμων. Προς τούτο, η Επιτροπή μπορεί επίσης να πραγματοποιεί τακτικές συναντήσεις με τις αρμόδιες εθνικές αρχές και άλλα ενδιαφερόμενα μέρη.

(23) Τα μέτρα που προβλέπονται στον παρόντα κανονισμό είναι σύμφωνα με τη γνώμη της επιτροπής επικοινωνιών,

ΕΞΕΔΩΣΕ ΤΟΝ ΠΑΡΟΝΤΑ ΚΑΝΟΝΙΣΜΟ:

Άρθρο 1

Πεδίο εφαρμογής

Ο παρών κανονισμός εφαρμόζεται στην κοινοποίηση των παραβιάσεων προσωπικών δεδομένων από τους παρόχους διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών (εφεξής «ο πάροχος»).

Άρθρο 2

Κοινοποίηση στην αρμόδια εθνική αρχή

1. Ο πάροχος κοινοποιεί στην αρμόδια εθνική αρχή όλες τις παραβιάσεις προσωπικών δεδομένων.

2. Ο πάροχος κοινοποιεί στην αρμόδια εθνική αρχή την παραβίαση προσωπικών δεδομένων το αργότερο 24 ώρες έπειτα από την ανίχνευση της παραβίασης προσωπικών δεδομένων, εφόσον αυτό είναι εφικτό.

Στην κοινοποίησή του προς την αρμόδια εθνική αρχή ο πάροχος περιλαμβάνει τις πληροφορίες που καθορίζονται στο παράρτημα I.

Η ανίχνευση παραβίασης προσωπικών δεδομένων θεωρείται ότι έχει πραγματοποιηθεί όταν ο πάροχος έχει αποκτήσει επαρκή επίγνωση ότι έχει συμβεί περιστατικό ασφάλειας με αποτέλεσμα διακύβευση δεδομένων προσωπικού χαρακτήρα, προκειμένου να συντάξει ουσιαστική ανακοίνωση, όπως απαιτείται βάσει του παρόντος κανονισμού.

3. Εφόσον δεν είναι διαθέσιμο το σύνολο των πληροφοριών που αναφέρονται στο παράρτημα I και απαιτείται περαιτέρω διερεύνηση της παραβίασης προσωπικών δεδομένων, επιτρέπεται στον πάροχο να προχωρήσει σε αρχική κοινοποίηση προς την αρμόδια εθνική αρχή το αργότερο 24 ώρες έπειτα από την ανίχνευση της παραβίασης προσωπικών δεδομένων. Η αρχική αυτή κοινοποίηση προς την αρμόδια εθνική αρχή περιλαμβάνει τις πληροφορίες που προβλέπονται στο τμήμα 1 του παραρτήματος I. Ο πάροχος προχωρεί σε δεύτερη κοινοποίηση προς την αρμόδια εθνική αρχή, το συντομότερο δυνατό, και το αργότερο εντός τριών ημερών από την αρχική κοινοποίηση. Η δεύτερη αυτή κοινοποίηση περιλαμβάνει τις πληροφορίες που προβλέπονται στο τμήμα 2 του παραρτήματος I και, κατά περίπτωση, τις ήδη παρασχεθείσες πληροφορίες.

Εφόσον ο πάροχος, παρά τις έρευνές του, δεν είναι σε θέση να παράσχει το σύνολο των πληροφοριών εντός της τριήμερης προθεσμίας από την αρχική κοινοποίηση, κοινοποιεί εντός του προβλεπόμενου χρονοδιαγράμματος τις πληροφορίες που διαθέτει και υποβάλλει στην αρμόδια εθνική αρχή τεκμηριωμένη αιτιολόγηση για την καθυστερημένη κοινοποίηση των υπόλοιπων πληροφοριών. Ο πάροχος κοινοποιεί στην αρμόδια εθνική αρχή τις υπόλοιπες πληροφορίες και, κατά περίπτωση, επικαιροποιεί τις ήδη παρασχεθείσες πληροφορίες, το συντομότερο δυνατό.

4. Η αρμόδια εθνική αρχή παρέχει σε όλους τους παρόχους που είναι εγκατεστημένοι στο συγκεκριμένο κράτος μέλος ασφαλές ηλεκτρονικό μέσο για την κοινοποίηση των παραβιάσεων προσωπικών δεδομένων, καθώς και πληροφορίες σχετικά με τις διαδικασίες για την πρόσβαση σε αυτό, καθώς και για τη χρήση του. Κατά περίπτωση, η Επιτροπή συγκαλεί συναντήσεις με τις αρμόδιες εθνικές αρχές προς διευκόλυνση της εφαρμογής της εν λόγω διάταξης.

5. Εφόσον η παραβίαση προσωπικών δεδομένων επηρεάζει συνδρομητές ή άτομα από κράτη μέλη εκτός αυτού της αρμόδιας εθνικής αρχής στην οποία έχει κοινοποιηθεί η παραβίαση προσωπικών δεδομένων, η αρμόδια εθνική αρχή ενημερώνει τις άλλες εθνικές αρχές.

Για να διευκολυνθεί η εφαρμογή της εν λόγω διάταξης, η Επιτροπή δημιουργεί και διατηρεί κατάλογο με τις αρμόδιες εθνικές αρχές και τα κατάλληλα σημεία επικοινωνίας.

Άρθρο 3

Κοινοποίηση στον συνδρομητή ή άτομο

1. Εφόσον η παραβίαση προσωπικών δεδομένων είναι πιθανό να επηρεάσει αρνητικά τα προσωπικά δεδομένα ή την ιδιωτική ζωή ενός συνδρομητή ή ατόμου, ο πάροχος, εκτός από την κοινοποίηση που αναφέρεται στο άρθρο 2, κοινοποιεί επίσης στον συνδρομητή ή το άτομο την παραβίαση.

2. Το κατά πόσο μια παραβίαση προσωπικών δεδομένων είναι πιθανό να επηρεάσει αρνητικά τα προσωπικά δεδομένα ή την ιδιωτική ζωή ενός συνδρομητή ή ατόμου, αξιολογείται λαμβάνοντας ιδίως υπόψη τις ακόλουθες περιστάσεις:

α) τον χαρακτήρα και το περιεχόμενο των εν λόγω δεδομένων προσωπικού χαρακτήρα, ιδίως εφόσον τα δεδομένα αφορούν οικονομικές πληροφορίες, ειδικές κατηγορίες δεδομένων που αναφέρονται στο άρθρο 8 παράγραφος 1 της οδηγίας 95/46/ΕΚ, καθώς και δεδομένα γεωγραφικής θέσης, διαδικτυακά αρχεία διαδικτυακής καταγραφής, ιστορικά ιστοπεριήγησης, στοιχεία ηλε-ταχυδρομείου, και αναλυτικούς καταλόγους κλήσεων·

β) τις πιθανές συνέπειες από την παραβίαση προσωπικών δεδομένων για τον ενδιαφερόμενο συνδρομητή ή άτομο, ιδίως εφόσον η παράβαση θα μπορούσε να συνεπάγεται κλοπή ταυτότητας ή απάτη, σωματική βλάβη, ψυχολογική πίεση, ταπείνωση ή προσβολή της υπολήψεως· και

γ) τις συνθήκες της παραβίασης προσωπικών δεδομένων, ιδίως εφόσον τα δεδομένα έχουν κλαπεί ή όταν ο πάροχος γνωρίζει ότι τα δεδομένα βρίσκονται στην κατοχή μη εξουσιοδοτημένου τρίτου.

3. Η κοινοποίηση στον συνδρομητή ή το άτομο γίνεται χωρίς αδικαιολόγητη καθυστέρηση ύστερα από την ανίχνευση της παραβίασης προσωπικών δεδομένων, όπως ορίζεται στο τρίτο εδάφιο του άρθρου 2 παράγραφος 2. Τούτο δεν εξαρτάται από την κοινοποίηση της παραβίασης προσωπικών δεδομένων στην αρμόδια εθνική αρχή, που αναφέρεται στο άρθρο 2.

4. Στην κοινοποίησή του προς τον συνδρομητή ή το άτομο, ο πάροχος περιλαμβάνει τις πληροφορίες που καθορίζονται στο παράρτημα II. Η κοινοποίηση στον συνδρομητή ή το άτομο διατυπώνεται με σαφή και εύληπτο τρόπο. Ο πάροχος δεν χρησιμοποιεί την κοινοποίηση ως ευκαιρία για προώθηση ή διαφήμιση νέων ή συμπληρωματικών υπηρεσιών.

5. Σε εξαιρετικές περιπτώσεις, εφόσον η κοινοποίηση στο συνδρομητή ή άτομο μπορεί να θέσει σε κίνδυνο την ορθή διερεύνηση της παραβίασης προσωπικών δεδομένων, επιτρέπεται στον πάροχο, αφού λάβει τη σύμφωνη γνώμη της αρμόδιας εθνικής αρχής, να καθυστερήσει την κοινοποίηση προς τον συνδρομητή ή άτομο έως ότου η αρμόδια εθνική αρχή θεωρήσει ότι είναι δυνατόν να κοινοποιήσει την παραβίαση προσωπικών δεδομένων, σύμφωνα με το εν λόγω άρθρο.

6. Ο πάροχος ενημερώνει τον συνδρομητή ή άτομο σχετικά με την παραβίαση προσωπικών δεδομένων με επικοινωνία που διασφαλίζει άμεση και ασφαλή παραλαβή των πληροφοριών, σύμφωνα με την εξέλιξη της τεχνολογίας. Οι πληροφορίες σχετικά με την παράβαση αφορούν αποκλειστικά την παράβαση και δεν σχετίζονται με πληροφορίες σχετικά με άλλο θέμα.

7. Εφόσον ο πάροχος που έχει άμεση συμβατική σχέση με τον τελικό χρήστη, παρά τις εύλογες προσπάθειές του, δεν είναι σε θέση να εντοπίσει εντός του χρονικού πλαισίου που αναφέρεται στην παράγραφο 3 όλα τα άτομα που είναι πιθανό να έχουν επηρεαστεί αρνητικά από την παραβίαση προσωπικών δεδομένων, μπορεί (ο πάροχος) να ειδοποιήσει τα άτομα αυτά με καταχώριση σε σημαντικά εθνικά ή περιφερειακά μέσα επικοινωνίας, στο αντίστοιχο κράτος μέλος, σε αυτό το χρονικό πλαίσιο. Αυτές οι καταχωρίσεις περιέχουν τις πληροφορίες που παρατίθενται στο παράρτημα II, όπου είναι απαραίτητο σε συνοπτική μορφή. Στην περίπτωση αυτή, ο πάροχος συνεχίζει να καταβάλλει κάθε εύλογη προσπάθεια για να εντοπίσει το συντομότερο τα άτομα αυτά και να τους κοινοποιήσει τις πληροφορίες που αναφέρονται στο παράρτημα II.

Άρθρο 4

Τεχνολογικά μέτρα προστασίας

1. Κατά παρέκκλιση από το άρθρο 3 παράγραφος 1, η κοινοποίηση παραβίασης προσωπικών δεδομένων σε ενδιαφερόμενο συνδρομητή ή άτομο δεν απαιτείται εάν ο πάροχος έχει αποδείξει κατά ικανοποιητικό τρόπο για την αρμόδια αρχή ότι έχει εφαρμόσει κατάλληλα τεχνολογικά μέτρα προστασίας και ότι τα μέτρα αυτά εφαρμόστηκαν ως προς τα δεδομένα που αφορούσε η παραβίαση της ασφάλειας. Τα εν λόγω τεχνολογικά μέτρα προστασίας πρέπει να καθιστούν τα δεδομένα ακατανόητα σε οποιοδήποτε πρόσωπο δεν διαθέτει δικαίωμα πρόσβασης σε αυτά.

2. Τα δεδομένα θεωρούνται ακατάληπτα, εάν:

α) έχουν κρυπτοθετηθεί με τυποποιημένο αλγόριθμο, το κλειδί που χρησιμοποιείται για την αποκρυπτοθέτηση των δεδομένων δεν έχει παραβιαστεί σε οποιαδήποτε παραβίαση της ασφάλειας, και το κλειδί που χρησιμοποιείται για την αποκρυπτοθέτηση των δεδομένων έχει δημιουργηθεί κατά τρόπο που να μην μπορεί να εξακριβωθεί με τα διαθέσιμα τεχνολογικά μέσα από οποιοδήποτε πρόσωπο που δεν έχει εξουσιοδοτημένη πρόσβαση στο κλειδί· ή

β) έχουν αντικατασταθεί από την τιμή κατακερματισμού τους, που έχει υπολογιστεί με τυποποιημένη κρυπτοθετημένη συνάρτηση κατακερματισμού, το κλειδί που χρησιμοποιείται για την αποκρυπτοθέτηση των δεδομένων δεν έχει παραβιαστεί σε οποιαδήποτε παραβίαση της ασφάλειας, και το κλειδί που χρησιμοποιείται για την αποκρυπτοθέτηση των δεδομένων έχει δημιουργηθεί κατά τρόπο που να μην μπορεί να εξακριβωθεί με τα διαθέσιμα τεχνολογικά μέσα από οποιοδήποτε πρόσωπο που δεν έχει εξουσιοδοτημένη πρόσβαση στο κλειδί.

3. Η Επιτροπή, έπειτα από διαβούλευση με τις αρμόδιες εθνικές αρχές μέσω της ομάδας εργασίας του άρθρου 29, τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια δικτύων και Πληροφοριών και τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων, μπορεί να δημοσιεύσει ενδεικτικό κατάλογο κατάλληλων τεχνολογικών μέτρων προστασίας που αναφέρονται στην παράγραφο 1, σύμφωνα με τρέχουσες πρακτικές.

Άρθρο 5

Χρησιμοποίηση άλλου παρόχου

Στις περιπτώσεις που συνάπτεται σύμβαση με άλλο πάροχο για την παροχή μέρους των υπηρεσιών ηλεκτρονικών επικοινωνιών χωρίς ο άλλος πάροχος να έχει άμεση συμβατική σχέση με τους συνδρομητές, ο εν λόγω άλλος πάροχος ενημερώνει αμέσως τον συμβατικό πάροχο σε περίπτωση παραβίασης προσωπικών δεδομένων.

Άρθρο 6

Υποβολή εκθέσεων και επανεξέταση

Εντός τριών ετών από την έναρξη ισχύος του παρόντος κανονισμού, η Επιτροπή υποβάλλει έκθεση σχετικά με την εφαρμογή του παρόντος κανονισμού, την αποτελεσματικότητά του και τον αντίκτυπό του σε παρόχους, συνδρομητές και ιδιώτες. Βάσει της εν λόγω έκθεσης, η Επιτροπή αναθεωρεί τον παρόντα κανονισμό.

Άρθρο 7

Έναρξη ισχύος

Ο παρών κανονισμός αρχίζει να ισχύει στις 25 Αυγούστου 2013.

Ο παρών κανονισμός είναι δεσμευτικός ως προς όλα τα μέρη του και ισχύει άμεσα σε κάθε κράτος μέλος.

Βρυξέλλες, 24 Ιουνίου 2013.

Για την Επιτροπή

Ο Πρόεδρος

José Manuel BARROSO

ΠΑΡΑΡΤΗΜΑ I

Περιεχόμενο της κοινοποίησης προς τις αρμόδιες εθνικές αρχές

Τμήμα 1

Ταυτοποίηση του παρόχου

1. Ονομασία του παρόχου

2. Ταυτότητα και στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων ή άλλου αρμόδιου επικοινωνίας από τον οποίο μπορούν να ληφθούν περισσότερες πληροφορίες·

3. Εάν πρόκειται για πρώτη ή δεύτερη κοινοποίηση

Αρχική πληροφόρηση σχετικά με την παραβίαση προσωπικών δεδομένων (προς συμπλήρωση σε μεταγενέστερες κοινοποιήσεις, κατά περίπτωση)

4. Ημερομηνία και ώρα του περιστατικού (εφόσον είναι γνωστές· εφόσον απαιτείται μπορεί να γίνει εκτίμηση) και της ανίχνευσης του περιστατικού

5. Περιστάσεις της παραβίασης προσωπικών δεδομένων (π.χ. απώλεια, κλοπή, αντιγραφή)

6. Χαρακτήρας και περιεχόμενο των σχετικών προσωπικών δεδομένων

7. Τεχνικά και οργανωτικά μέτρα που ελήφθησαν (ή που θα ληφθούν) από τον πάροχο όσο αφορά τα θιγόμενα προσωπικά δεδομένα

8. Σχετική χρήση άλλου παρόχου (όπου ισχύει)

Τμήμα 2

Περαιτέρω πληροφορίες σχετικά με την παραβίαση προσωπικών δεδομένων

9. Περίληψη του συμβάντος που προκάλεσε την παραβίαση προσωπικών δεδομένων (συμπεριλαμβανομένης της γεωγραφικής θέσης της παραβίασης και των εμπλεκόμενων μέσων αποθήκευσης):

10. Αριθμός θιγόμενων συνδρομητών ή ατόμων

11. Δυνητικές συνέπειες και δυνητικά δυσμενείς επιπτώσεις σε συνδρομητές ή άτομα

12. Τεχνικά και οργανωτικά μέτρα που έλαβε ο πάροχος για την άμβλυνση δυνητικά δυσμενών επιπτώσεων

Πιθανή πρόσθετη κοινοποίηση σε συνδρομητές ή άτομα

13. Περιεχόμενο της κοινοποίησης

14. Μέσα επικοινωνίας που χρησιμοποιήθηκαν

15. Αριθμός συνδρομητών ή ατόμων που έχουν ενημερωθεί

Πιθανά διασυνοριακά θέματα

16. Παραβίαση προσωπικών δεδομένων που αφορά συνδρομητές ή άτομα σε άλλα κράτη μέλη

17. Κοινοποίηση σε άλλες αρμόδιες εθνικές αρχές

ΠΑΡΑΡΤΗΜΑ II

Περιεχόμενο της κοινοποίησης προς τον συνδρομητή ή άτομο

1. Ονομασία του παρόχου

2. Ταυτότητα και στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων ή άλλου αρμόδιου επικοινωνίας από τον οποίο μπορούν να ληφθούν περισσότερες πληροφορίες

3. Σύνοψη του περιστατικού που προξένησε την παραβίαση προσωπικών δεδομένων

4. Εκτιμώμενη ημερομηνία του περιστατικού

5. Χαρακτήρας και περιεχόμενο των σχετικών προσωπικών δεδομένων όπως αναφέρεται στο άρθρο 3 παράγραφος 2

6. Πιθανές συνέπειες από την παραβίαση προσωπικών δεδομένων για τον θιγόμενο συνδρομητή ή άτομο, όπως αναφέρεται στο άρθρο 3 παράγραφος 2

7. Περιστάσεις της παραβίασης προσωπικών δεδομένων όπως αναφέρεται στο άρθρο 3 παράγραφος 2

8. Μέτρα που έλαβε ο πάροχος προς αντιμετώπιση της παραβίασης προσωπικών δεδομένων

9. Συνιστώμενα από τον πάροχο μέτρα για άμβλυνση πιθανών δυσμενών επιπτώσεων