

# Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft

## Πεδίο εφαρμογής

Οι Απαιτήσεις προστασίας δεδομένων («ΑΠΔ») προμηθευτών της Microsoft ισχύουν για κάθε προμηθευτή της Microsoft που επεξεργάζεται Προσωπικά δεδομένα ή Εμπιστευτικά δεδομένα της Microsoft τα οποία σχετίζονται με την εκτέλεση καθηκόντων του συγκεκριμένου προμηθευτή (π.χ. παροχή υπηρεσιών, άδειες χρήσης λογισμικού, υπηρεσίες cloud) σύμφωνα με τους όρους της σύμβασής του με τη Microsoft (π.χ. όροι εντολών αγοράς, κύρια συμφωνία) («**Εκτέλεση καθηκόντων**»).

- Σε περίπτωση διαφωνίας μεταξύ των ΑΠΔ και των απαιτήσεων που ορίζονται στις συμβατικές συμφωνίες μεταξύ του προμηθευτή και της Microsoft, οι ΑΠΔ υπερισχύουν, εκτός εάν ο προμηθευτής προσδιορίσει την ορθή διάταξη στη σύμβαση που αντικαθιστά την ισχύουσα απαίτηση προστασίας δεδομένων (στην περίπτωση αυτή, οι όροι της σύμβασης υπερισχύουν).
- Σε περίπτωση διαφωνίας μεταξύ των απαιτήσεων που περιέχονται στο παρόν έγγραφο και τυχόν νομικών ή θεσμοθετημένων απαιτήσεων, υπερισχύουν οι νομικές ή θεσμοθετημένες απαιτήσεις.
- Σε περίπτωση που ο προμηθευτής της Microsoft είναι Υπεύθυνος Επεξεργασίας, ο προμηθευτής ενδέχεται να έχει μειωμένες απαιτήσεις στις ΑΠΔ.
- Σε περίπτωση που ο προμηθευτής της Microsoft δεν επεξεργάζεται προσωπικά δεδομένα της Microsoft αλλά μόνο εμπιστευτικά δεδομένα της Microsoft, σε σχέση με τις παρούσες ΑΠΔ, ο προμηθευτής ενδέχεται να έχει μειωμένες απαιτήσεις.

## Διεθνής μετάδοση δεδομένων

Χωρίς να περιορίζει τις άλλες υποχρεώσεις του, ο προμηθευτής δεν θα προβεί σε διεθνή μετάδοση Προσωπικών δεδομένων της Microsoft εκτός εάν η Microsoft έχει παράσχει πρότερη γραπτή έγκριση και, σε κάθε περίπτωση, ο προμηθευτής θα συμμορφώνεται με τις Απαιτήσεις προστασίας δεδομένων, συμπεριλαμβανομένων των Τυπικών συμβατικών ρητρών, ή, κατά την κρίση της Microsoft, με άλλους κατάλληλους μηχανισμούς διασυνοριακής μεταφοράς που έχουν εγκριθεί από την κατάλληλη αρχή προστασίας δεδομένων ή την Ευρωπαϊκή Επιτροπή, κατά περίπτωση, και έχουν εγκριθεί ή συμφωνηθεί από τη Microsoft. Διάδοχες τυπικές συμβατικές ρήτρες που έχουν υιοθετηθεί από (i) την Ευρωπαϊκή Επιτροπή ή έχουν υιοθετηθεί από τον Ευρωπαϊκό Επόπτη Προστασίας Δεδομένων και έχουν εγκριθεί από την Ευρωπαϊκή Επιτροπή, (ii) το Ηνωμένο Βασίλειο σύμφωνα με τον Γενικό Ομοσπονδιακό Νόμο περί προστασίας δεδομένων του ΗΒ, (iii) την Ελβετία σύμφωνα με τον ελβετικό Ομοσπονδιακό Νόμο περί προστασίας δεδομένων, ή (iv) ρήτρες που διέπουν τη διεθνή μετάδοση δεδομένων προσωπικού χαρακτήρα που έχουν υιοθετηθεί επίσημα από κυβέρνηση σε δικαιοδοσία διαφορετική από την Ελβετία, το Ηνωμένο Βασίλειο και τις δικαιοδοσίες που αποτελούν την Ευρωπαϊκή Ένωση ή τον Ευρωπαϊκό Οικονομικό Χώρο, θα ενσωματωθούν και δεσμεύουν τον Προμηθευτή από την ημέρα της υιοθέτησής τους. Ο Προμηθευτής θα εξασφαλίζει επίσης ότι συμμορφώνονται όλοι και οποιοδήποτε υπεργολάβοι επεξεργασίας (όπως ορίζονται στις Τυπικές συμβατικές ρήτρες).

## Βασικοί ορισμοί

Οι ακόλουθοι όροι που χρησιμοποιούνται σε αυτές τις ΑΠΔ έχουν τις ακόλουθες έννοιες. Οι λίστες παραδειγμάτων που ακολουθούν τις λέξεις «συμπεριλαμβανομένων», «όπως», «π.χ.», «για παράδειγμα» ή παρόμοιες λέξεις που χρησιμοποιούνται σε όλο το έγγραφο αυτών των ΑΠΔ ερμηνεύονται σαν να περιλαμβάνουν τις λέξεις «χωρίς περιορισμό» ή «ενδεικτικά» εκτός εάν χαρακτηρίζονται από λέξεις όπως «μόνο» ή «αποκλειστικά». Για περαιτέρω ορισμούς, ανατρέξτε στο Γλωσσάρι που βρίσκεται στο τέλος αυτού του εγγράφου.

Ως «**Υπεύθυνος Επεξεργασίας**» νοείται η οντότητα που καθορίζει τους σκοπούς και τα μέσα της Επεξεργασίας Προσωπικών δεδομένων. Ο «Υπεύθυνος Επεξεργασίας» περιλαμβάνει μια επιχείρηση, έναν υπεύθυνο επεξεργασίας (όπως αυτός ο όρος ορίζεται στον ΓΚΠΔ) και ισοδύναμους όρους στους Νόμους περί προστασίας δεδομένων, όπως απαιτεί το πλαίσιο.

Τα «**cookie**» είναι μικρά αρχεία κειμένου που αποθηκεύονται σε συσκευές από ιστοτόπους ή/και εφαρμογές που περιέχουν πληροφορίες οι οποίες χρησιμοποιούνται για αναγνώριση ενός υποκειμένου δεδομένων ή μιας συσκευής.

Με τον όρο «**Περιστατικό παραβίασης δεδομένων**» νοείται (1) μια παραβίαση ασφάλειας που οδήγησε σε ακούσια ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη γνωστοποίηση ή πρόσβαση σε Προσωπικά δεδομένα Microsoft ή

Εμπιστευτικά δεδομένα Microsoft που έχουν μεταδοθεί, αποθηκευτεί ή με άλλον τρόπο υποστεί επεξεργασία από τον Προμηθευτή ή τους Υπεργολάβους του, ή (2) ευπάθεια ασφάλειας που σχετίζεται με τον χειρισμό από τον Προμηθευτή των Προσωπικών δεδομένων Microsoft ή των Εμπιστευτικών δεδομένων Microsoft.

«**Υποκείμενο δεδομένων**» σημαίνει ένα αναγνωρίσιμο φυσικό πρόσωπο το οποίο μπορεί να ταυτοποιηθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς αναγνωριστικού όπως όνομα, αριθμό αναγνώρισης, δεδομένα τοποθεσίας, διαδικτυακό αναγνωριστικό, ή με βάση ενός ή περισσότερων παραγόντων που αφορούν τη σωματική, φυσιολογική, γενετική, ψυχική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα αυτού του φυσικού προσώπου.

Με τον όρο «**Δικαίωμα υποκειμένου δεδομένων**» νοείται το δικαίωμα ενός Υποκειμένου δεδομένων για πρόσβαση, διαγραφή, επεξεργασία, εξαγωγή, περιορισμό ή ένσταση στην Επεξεργασία προσωπικών δεδομένων από τη Microsoft του συγκεκριμένου Υποκειμένου δεδομένων όπως απαιτείται από τη Νομοθεσία.

Με τον όρο «**Νομοθεσία**» νοείται κάθε εφαρμοστέος νόμος, κανόνας, διάταγμα, νομοθέτημα, απόφαση, εντολή, κανονισμός, κρίση, κώδικας, θέσπισμα, αποφάσεις και απαιτήσεις από οποιαδήποτε κρατική αρχή (ομοσπονδιακή, πολιτειακή, τοπική ή διεθνή) που έχει δικαιοδοσία. Με τον όρο «**Παράνομο**» νοείται οποιαδήποτε παράβαση της Νομοθεσίας.

Με τον όρο «**Εμπιστευτικά δεδομένα της Microsoft**» νοούνται όλες οι πληροφορίες οι οποίες, εάν διαρρεύσουν λόγω ζητημάτων εμπιστευτικότητας ή ακεραιότητας, ενδέχεται να προκαλέσουν σημαντικές απώλειες αξιοπιστίας ή εσόδων στη Microsoft. Σε αυτά τα δεδομένα περιλαμβάνονται προϊόντα υλικού και λογισμικού της Microsoft, εσωτερικές επιχειρησιακές εφαρμογές, αδημοσίευτο υλικό μάρκετινγκ, αριθμοί-κλειδιά αδειών χρήσης προϊόντων, και τεχνική τεκμηρίωση που σχετίζεται με τα προϊόντα και τις υπηρεσίες της Microsoft.

Με τον όρο «**Προσωπικά δεδομένα της Microsoft**» νοούνται οποιαδήποτε Προσωπικά δεδομένα που έχουν υποβληθεί σε Επεξεργασία από τη Microsoft ή εκ μέρους της.

Με τον όρο «**Προσωπικά δεδομένα**» νοούνται οι πληροφορίες που σχετίζονται με ένα Υποκείμενο δεδομένων και άλλες πληροφορίες που αποτελούν «προσωπικά δεδομένα» ή «προσωπικές πληροφορίες» σύμφωνα με τον Νόμο.

Με τον όρο «**Επεξεργασία**» νοείται οποιαδήποτε λειτουργία ή σύνολο λειτουργιών που εκτελείται στα Προσωπικά δεδομένα ή Εμπιστευτικά δεδομένα της Microsoft, με αυτοματοποιημένα ή μη μέσα, όπως η συλλογή, η εγγραφή, η οργάνωση, η δόμηση, η αποθήκευση, η προσαρμογή ή η αλλοίωση, η ανάκτηση, η διαβούλευση, η χρήση, η γνωστοποίηση μέσω μετάδοσης, η διάδοση ή η με οποιονδήποτε άλλο τρόπο διάθεση, ευθυγράμμιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή. Οι όροι «Σε επεξεργασία» και «Υπό επεξεργασία» θα έχουν τις αντίστοιχες σημασίες.

«**Υπεύθυνος Επεξεργασίας**» σημαίνει μια οντότητα που επεξεργάζεται Προσωπικά δεδομένα για λογαριασμό άλλης οντότητας και περιλαμβάνει Πάροχο Υπηρεσιών, Υπεύθυνο Επεξεργασίας (όπως αυτός ο όρος ορίζεται στον ΓΚΠΔ) και ισοδύναμους όρους στους Νόμους περί προστασίας δεδομένων, όπως απαιτείται από το θεματικό περιβάλλον.

Με τον όρο «**Υπεργολάβος**» νοείται ένα τρίτο μέρος στο οποίο ο προμηθευτής μεταβιβάζει τις υποχρεώσεις του με βάση τη σύμβαση που καλύπτει την Εκτέλεση καθκόντων, συμπεριλαμβανομένων των συγγενών εταιρειών του προμηθευτή που δεν διαθέτουν άμεση σύμβαση με τη Microsoft.

Με τον όρο «**Υπεργολάβος Επεξεργασίας**» νοείται ένα τρίτο μέρος το οποίο η Microsoft δεσμεύει για Εκτέλεση καθκόντων, όπου η Εκτέλεση καθκόντων περιλαμβάνει Επεξεργασία προσωπικών δεδομένων της Microsoft για τα οποία η Microsoft είναι Υπεύθυνος Επεξεργασίας.

## Απόκριση προμηθευτή

Οι προμηθευτές επιβεβαιώνουν τη συμμόρφωση με τις παρούσες απαιτήσεις ετησίως χρησιμοποιώντας μια διαδικτυακή υπηρεσία που διαχειρίζεται η Microsoft. Ανατρέξτε στον [Οδηγό Προγράμματος SSPA](#) για να κατανοήσετε τον τρόπο διαχείρισης της συμμόρφωσης.

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα Α: Διαχείριση</b>		
1	<p>Κάθε ισχύουσα σύμβαση μεταξύ της Microsoft και του προμηθευτή (π.χ. κύρια συμφωνία, πρόταση εργασίας, εντολές αγοράς και άλλες εντολές) περιέχει διατύπωση για την προστασία δεδομένων σχετικά με το απόρρητο και την ασφάλεια προστασίας προσωπικών δεδομένων αναφορικά με τα Εμπιστευτικά και Προσωπικά δεδομένα της Microsoft, κατά περίπτωση, συμπεριλαμβανομένων των απαγορεύσεων για την πώληση Προσωπικών δεδομένων της Microsoft και την Επεξεργασία προσωπικών δεδομένων της Microsoft εκτός της άμεσης επιχειρηματικής σχέσης μεταξύ της Microsoft και του προμηθευτή.</p> <p>Για εταιρείες που λειτουργούν ως Υπεύθυνοι Επεξεργασίας ή Υπεργολάβοι Επεξεργασίας σε σχέση με την Εκτέλεση καθηκόντων, όσον αφορά τα Προσωπικά δεδομένα της Microsoft, η σύμβαση πρέπει να συμπεριλαμβάνει το αντικείμενο και τη διάρκεια της Επεξεργασίας, τη φύση και τον σκοπό της Επεξεργασίας, τον τύπο των Προσωπικών δεδομένων της Microsoft και τις κατηγορίες των Υποκειμένων δεδομένων, και τις υποχρεώσεις και τα δικαιώματα της Microsoft.</p>	<p>Ο Προμηθευτής οφείλει να παρουσιάσει την ισχύουσα σύμβαση μεταξύ της Microsoft και του Προμηθευτή.</p> <p>Για τους Υπεύθυνους Επεξεργασίας και τους Υπεργολάβους Επεξεργασίας, οι περιγραφές Επεξεργασίας περιέχονται στην ισχύουσα σύμβαση (π.χ. πρόταση εργασίας, εντολές αγοράς).</p> <p>Σημείωση: Για τις εταιρείες με εντολές αγοράς που έχουν επιβεβαιωθεί αλλά δεν έχουν ακόμα εκπληρωθεί, η απαραίτητη περιγραφή δραστηριοτήτων Επεξεργασίας μπορεί να προστεθεί αργότερα στη διαδικασία αγοράς.</p>
2	<p>Σε περίπτωση που η Microsoft επιβεβαιώσει ότι οι δεσμεύσεις σας εκπληρώνουν έναν ρόλο Υπεργολάβου Επεξεργασίας, ο Προμηθευτής πρέπει να έχει συνάψει ισχύουσες συμφωνίες προστασίας δεδομένων με τη Microsoft.</p> <p>Σημείωση: Η Microsoft θα δημοσιεύσει αυτήν την ένδειξη στο προφίλ σας μόλις αυτό ισχύσει.</p>	<p>Τυπικές συμβατικές ρήτρες, Προσάρτημα περί Διαδικτυακών δεδομένων πελατών ή/και Προσάρτημα περί Επεξεργασίας δεδομένων επαγγελματικών υπηρεσιών προμηθευτών και συνεργατών.</p>
3	<p>Ανάθεση της ευθύνης και της λογοδοσίας όσον αφορά τη συμμόρφωση με τις απαιτήσεις ΑΠΔ σε ένα κατονομαζόμενο πρόσωπο ή ομάδα στην εταιρεία.</p>	<p>Ονομάστε τον ρόλο του ατόμου ή της ομάδας που είναι επιφορτισμένη με τη διασφάλιση της συμμόρφωσης με τις ΑΠΔ προμηθευτών της Microsoft.</p> <p>Ένα έγγραφο που περιγράφει την εξουσία και τη λογοδοσία αυτού του ατόμου ή της ομάδας που καταδεικνύει έναν ρόλο απορρήτου ή/και ασφάλειας.</p>
4	<p>Καθιέρωση, διατήρηση και εκτέλεση ετήσιας εκπαίδευσης απορρήτου και ασφάλειας για υπαλλήλους που θα έχουν πρόσβαση στα Προσωπικά δεδομένα που επεξεργάζεται ο προμηθευτής σε σχέση με την Εκτέλεση καθηκόντων ή τα Εμπιστευτικά δεδομένα της Microsoft .</p> <p>Εάν η εταιρεία σας δεν έχει έτοιμο περιεχόμενο, μπορείτε να χρησιμοποιήσετε αυτήν τη <a href="#">διάρθρωση εικονοσεναρίου</a> και να την προσαρμόσετε για την εταιρεία σας.</p> <p>Σημείωση: Ενδέχεται να απαιτηθεί από το προσωπικό του Προμηθευτή η ολοκλήρωση πρόσθετων εκπαιδευτικών προγραμμάτων που παρέχονται από τμήματα της Microsoft.</p>	<p>Διατίθενται ετήσια αρχεία παρακολούθησης, τα οποία μπορούν να παρασχεθούν στη Microsoft κατόπιν αιτήματος.</p> <p>Το εκπαιδευτικό περιεχόμενο περιλαμβάνει αρχές προστασίας προσωπικών δεδομένων και ασφάλειας.</p> <p>Η τεκμηρίωση της συμμόρφωσης με τις απαιτήσεις εκπαίδευσης θα περιλαμβάνει αποδεικτικά εκπαίδευσης που σχετίζεται με κανονιστικές απαιτήσεις προστασίας προσωπικών δεδομένων, υποχρεώσεις ασφάλειας, και συμμόρφωση με ισχύουσες συμβατικές απαιτήσεις και υποχρεώσεις.</p>

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα Α: Διαχείριση (συνέχ.)</b>		
5	<p>Επεξεργασία των Προσωπικών δεδομένων της Microsoft μόνο σύμφωνα με τις τεκμηριωμένες οδηγίες της Microsoft, συμπεριλαμβανομένων των σεναρίων σχετικά με τις μεταβιβάσεις Προσωπικών δεδομένων της Microsoft σε μία τρίτη χώρα ή έναν διεθνή οργανισμό, εκτός εάν αυτό απαιτείται από τη νομοθεσία. Σε τέτοια περίπτωση, ο Υπεύθυνος Επεξεργασίας ή ο Υπεργολάβος Επεξεργασίας (Προμηθευτής) πρέπει να ενημερώσει τον Υπεύθυνο Επεξεργασίας (Microsoft) για αυτήν τη νομική απαίτηση πριν από την επεξεργασία, εκτός εάν ο νόμος απαγορεύει τέτοιες πληροφορίες για σημαντικούς λόγους δημοσίου συμφέροντος.</p>	<p>Ο Προμηθευτής συγκεντρώνει και διατηρεί όλες τις τεκμηριωμένες οδηγίες της Microsoft (π.χ. συμφωνία, δήλωση εργασίας ή τεκμηρίωση εντολής αγοράς) ηλεκτρονικά, σε μια εύκολα προσβάσιμη τοποθεσία για τους υπαλλήλους του προμηθευτή και τους εργολάβους που συμμετέχουν στην Εκτέλεση καθηκόντων.</p>
<b>Ενότητα Β: Ειδοποίηση</b>		
6	<p>Ο προμηθευτής πρέπει να χρησιμοποιεί τη Δήλωση προστασίας προσωπικών δεδομένων της Microsoft, όταν συλλέγει Προσωπικά δεδομένα για λογαριασμό της Microsoft.</p> <p>Η ειδοποίηση προστασίας προσωπικών δεδομένων πρέπει να είναι εμφανής και διαθέσιμη στα Υποκείμενα δεδομένων, ώστε να τα βοηθήσει να αποφασίσουν αν θα υποβάλουν τα Προσωπικά δεδομένα τους στον προμηθευτή.</p> <p>Σημείωση: Σε περίπτωση όπου η εταιρεία σας είναι ο Υπεύθυνος της δραστηριότητας Επεξεργασίας, θα δημοσιεύσετε τη δική σας ειδοποίηση προστασίας προσωπικών δεδομένων.</p>	<p>Ο Προμηθευτής χρησιμοποιεί έναν σύνδεσμο <a href="#">fwdlink</a> προς την τρέχουσα, δημοσιευμένη Δήλωση προστασίας προσωπικών δεδομένων της Microsoft.</p> <p>Η Δήλωση προστασίας προσωπικών δεδομένων δημοσιεύεται σε οποιοδήποτε περιβάλλον στο οποίο πρόκειται να συλλέγονται Προσωπικά δεδομένα του χρήστη.</p> <p>Εφόσον ισχύει, διατίθεται μια έκδοση εκτός σύνδεσης και παρέχεται πριν από τη συλλογή δεδομένων.</p> <p>Οποιαδήποτε Δήλωση προστασίας προσωπικών δεδομένων εκτός σύνδεσης που χρησιμοποιείται είναι η πιο πρόσφατη, δημοσιευμένη έκδοση και φέρει τη σωστή ημερομηνία. Για υπηρεσίες εργαζομένων της Microsoft, χρησιμοποιείται η Ειδοποίηση προστασίας προσωπικών δεδομένων της Microsoft.</p>
7	<p>Κατά τη συλλογή Προσωπικών δεδομένων της Microsoft μέσω φωνητικής κλήσης σε πραγματικό χρόνο ή ηχογραφημένης φωνητικής κλήσης, οι προμηθευτές πρέπει να είναι έτοιμοι να συζητήσουν τις σχετικές πρακτικές συλλογής, χειρισμού, χρήσης και διατήρησης δεδομένων με τα Υποκείμενα δεδομένων.</p>	<p>Ένα σενάριο για τις φωνητικές ηχογραφήσεις περιλαμβάνει τον τρόπο Επεξεργασίας προσωπικών δεδομένων της Microsoft, καθώς και τα εξής:</p> <ul style="list-style-type: none"> <li>▪ συλλογή,</li> <li>▪ χρήση και</li> <li>▪ διατήρηση</li> </ul>

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα Γ: Επιλογή και συναίνεση</b>		
8	<p>Κατά περίπτωση, ο προμηθευτής πρέπει να λάβει και να καταγράψει τη συναίνεση ενός Υποκειμένου δεδομένων για όλες τις δραστηριότητες Επεξεργασίας του (συμπεριλαμβανομένων τυχόν νέων και ενημερωμένων δραστηριοτήτων Επεξεργασίας) πριν από τη συλλογή των Προσωπικών δεδομένων αυτού του Υποκειμένου δεδομένων.</p> <p>Ο Προμηθευτής παρακολουθεί την αποτελεσματικότητα της διαχείρισης προτιμήσεων προκειμένου να διασφαλίζει ότι το χρονοδιάγραμμα τήρησης μιας αλλαγής προτίμησης είναι η πιο περιοριστική τοπική νομική απαίτηση που ισχύει.</p>	<p>Ο Προμηθευτής μπορεί να επιδείξει τον τρόπο που ένα Υποκείμενο δεδομένων παρέχει συναίνεση για μια δραστηριότητα Επεξεργασίας και ότι το εύρος της συναίνεσης καλύπτει όλες τις δραστηριότητες Επεξεργασίας του προμηθευτή σε σχέση με τα Προσωπικά δεδομένα αυτού του Υποκειμένου δεδομένων.</p> <p>Ο προμηθευτής μπορεί να επιδείξει τον τρόπο με τον οποίο ένα Υποκείμενο δεδομένων αποσύρει τη συναίνεση για μια δραστηριότητα Επεξεργασίας.</p> <p>Ο προμηθευτής μπορεί να επιδείξει πώς ελέγχονται οι προτιμήσεις πριν από την εκκίνηση μιας νέας δραστηριότητας Επεξεργασίας.</p> <p>Σημείωση: Ως αποδεικτικά μπορούν να χρησιμοποιηθούν στιγμιότυπα οθόνης αλληλεπιδράσεων με χρήστες, πειραματισμοί με την υπηρεσία ή η ευκαιρία προβολής τεχνικής τεκμηρίωσης.</p>
9	<p>Οι προμηθευτές που δημιουργούν και διαχειρίζονται τοποθεσίες web ή/και εφαρμογές της Microsoft πρέπει να διασφαλίζουν ότι η χρήση των cookie συμβαδίζει με τις δεσμεύσεις στη Δήλωση προστασίας προσωπικών δεδομένων της Microsoft και με τις τοπικές νομικές απαιτήσεις.</p> <p>Εκτός εάν ζητηθεί ρητά το αντίθετο από τη συμβαλλόμενη επιχειρηματική μονάδα, οι προμηθευτές πρέπει να χρησιμοποιούν το Τυπικό μπάνερ που παράγεται από την 1ES για διαχείριση των χειριστηρίων επιλογής.</p> <p>Αυτή η απαίτηση ισχύει όταν οι ιστότοποι στοχεύουν χρήστες εντός της Ευρωπαϊκής Ένωσης/Ευρωπαϊκού Οικονομικού Χώρου και άλλων περιοχών με την ισχύουσα νομοθεσία περί προστασίας προσωπικών δεδομένων και οπουδήποτε χρησιμοποιείται η Δήλωση προστασίας προσωπικών δεδομένων της Microsoft.</p> <p>Σημείωση: Οι επιχειρηματικοί χορηγοί της Microsoft πρέπει να εγγράψουν τους ιστοτόπους Web της Microsoft στην εσωτερική πύλη Συμμόρφωσης Web (<a href="http://aka.ms/wcp">http://aka.ms/wcp</a>), για καταλογοποίηση και διαχείριση του αποθέματος cookie.</p>	<p>Ο σκοπός κάθε cookie πρέπει να τεκμηριώνεται και να αναφέρει τον τύπο cookie που έχει υλοποιηθεί.</p> <ul style="list-style-type: none"> <li>▪ Δεν πρέπει να χρησιμοποιούνται μόνιμα cookie σε περιπτώσεις όπου επαρκούν τα cookie περιόδου λειτουργίας.</li> <li>▪ Όταν χρησιμοποιούνται μόνιμα cookie, δεν πρέπει να διαθέτουν ημερομηνία λήξης η οποία υπερβαίνει τους 13 μήνες από την επίσκεψη ενός χρήστη στην τοποθεσία.</li> </ul> <p>Επικυρώστε τη συμμόρφωση με τη Νομοθεσία της ΕΕ κατά περίπτωση, όπως:</p> <ul style="list-style-type: none"> <li>▪ χρήση της σύμβασης σήμανσης «Προστασία προσωπικών δεδομένων και cookie» για τη δήλωση προστασίας προσωπικών δεδομένων,</li> <li>▪ εξασφάλιση της συναίνεσης του χρήστη πριν από τη χρήση cookie για «μη ουσιαστικούς σκοπούς», όπως η διαφήμιση, και</li> <li>▪ η συναίνεση πρέπει να λήγει ή να εξασφαλιστεί εκ νέου σε διάστημα μικρότερο από 6 μήνες.</li> </ul>

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα Δ: Συλλογή</b>		
10	Ο προμηθευτής πρέπει να εποπτεύει τη συλλογή Προσωπικών ή/και Εμπιστευτικών δεδομένων της Microsoft, για να διασφαλίζει ότι τα μόνα δεδομένα που συλλέγονται είναι αυτά που απαιτούνται για την Εκτέλεση καθηκόντων.	<p>Ο προμηθευτής μπορεί να παράσχει τεκμηρίωση που δείχνει ότι τα Προσωπικά ή/και Εμπιστευτικά δεδομένα της Microsoft που συλλέγονται απαιτούνται για την Εκτέλεση καθηκόντων.</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
11	Πριν από τη συλλογή δεδομένων από παιδιά (όπως ορίζεται από την ισχύουσα δικαιοδοσία), ο Προμηθευτής πρέπει να λάβει τη συναίνεση σύμφωνα με την τοπική νομοθεσία περί Προστασίας προσωπικών δεδομένων.	<p>Ο Προμηθευτής μπορεί να παρέχει τεκμηρίωση που δείχνει τη συναίνεση γονέα/κηδεμόνα.</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
<b>Ενότητα Ε: Διατήρηση</b>		
12	Πρέπει να διασφαλίζεται ότι τα Προσωπικά και Εμπιστευτικά δεδομένα της Microsoft δεν διατηρούνται για περισσότερο χρόνο από αυτόν που είναι απαραίτητος για την Εκτέλεση καθηκόντων, εκτός εάν απαιτείται συνέχιση της διατήρησης των Προσωπικών ή/και Εμπιστευτικών δεδομένων της Microsoft από τη Νομοθεσία.	<p>Ο προμηθευτής συμμορφώνεται με τις τεκμηριωμένες πολιτικές διατήρησης ή απαιτήσεις διατήρησης που καθορίζονται από τη Microsoft στη σύμβαση (π.χ. πρόταση εργασίας, εντολή αγοράς).</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
13	<p>Πρέπει να διασφαλίζεται ότι, κατά την αποκλειστική διακριτική ευχέρεια της Microsoft, τα Προσωπικά και Εμπιστευτικά δεδομένα της Microsoft στην κατοχή του προμηθευτή ή υπό τον έλεγχο αυτού θα επιστρέφονται στη Microsoft ή θα καταστρέφονται μετά την ολοκλήρωση της Εκτέλεσης καθηκόντων ή κατόπιν αιτήματος της Microsoft.</p> <p>Οι εφαρμογές πρέπει να περιλαμβάνουν διαδικασίες που θα διασφαλίζουν ότι, όταν καταργούνται δεδομένα από την εφαρμογή, είτε ρητά από χρήστες είτε βάσει άλλων ενουσμάτων όπως είναι η ηλικία των δεδομένων, θα πρέπει να διαγράφονται με ασφάλεια.</p> <p>Όταν είναι απαραίτητη η καταστροφή Προσωπικών ή Εμπιστευτικών δεδομένων της Microsoft, ο προμηθευτής πρέπει να καίει, να κονιορτοποιεί ή να τεμαχίζει φυσικούς πόρους που περιέχουν Προσωπικά ή/και Εμπιστευτικά δεδομένα της Microsoft, ώστε να μην είναι δυνατή η ανάγνωση ή η ανασύσταση των πληροφοριών.</p>	<p>Διατηρήστε ένα αρχείο από την απόρριψη Προσωπικών και Εμπιστευτικών δεδομένων της Microsoft (αυτό μπορεί να περιλαμβάνει την επιστροφή στη Microsoft για καταστροφή).</p> <p>Εάν απαιτείται η καταστροφή ή αν ζητηθεί από τη Microsoft, παράσχετε ένα πιστοποιητικό καταστροφής με την υπογραφή ενός στελέχους του προμηθευτή.</p>



#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα ΣΤ: Υποκείμενα δεδομένων</b>		
	<p>Τα Υποκείμενα δεδομένων έχουν συγκεκριμένα δικαιώματα βάσει της Νομοθεσίας, συμπεριλαμβανομένου του δικαιώματος πρόσβασης, διαγραφής, επεξεργασίας, εξαγωγής, περιορισμού και ένστασης στην Επεξεργασία των Προσωπικών δεδομένων τους («<b>Δικαιώματα Υποκειμένων δεδομένων</b>»). Όταν ένα Υποκείμενο δεδομένων επιχειρεί να ασκήσει τα δικαιώματά του βάσει της Νομοθεσίας αναφορικά με τα Προσωπικά δεδομένα της Microsoft που του ανήκουν, ο προμηθευτής πρέπει να παρέχει τη δυνατότητα στη Microsoft να κάνει τα εξής ή να εκτελέσει αυτές τις ενέργειες για λογαριασμό της Microsoft:</p>	
14	<p>Υποστήριξη της Microsoft, μέσω κατάλληλων τεχνικών και οργανωτικών μέτρων, όπου είναι δυνατό, να εκπληρώσει τις υποχρεώσεις της για ανταπόκριση σε αιτήσεις των Υποκειμένων δεδομένων που προσπαθούν να ασκήσουν τα Δικαιώματα υποκειμένων δεδομένων χωρίς αδικαιολόγητη καθυστέρηση.</p> <p>Εκτός εάν του δοθούν διαφορετικές οδηγίες από τη Microsoft, ο Προμηθευτής θα παραπέμπει όλα τα Υποκείμενα δεδομένων που επικοινωνούν με τον Προμηθευτή απευθείας στη Microsoft, για να ασκήσουν τα Δικαιώματα υποκειμένων δεδομένων.</p>	<p>Ο προμηθευτής θα διατηρεί αποδεικτικά των τεκμηριωμένων διεργασιών και διαδικασιών για υποστήριξη της άσκησης των Δικαιωμάτων υποκειμένων δεδομένων.</p> <p>Ο προμηθευτής θα διατηρεί τεκμηριωμένα αποδεικτικά δοκιμών. Τα αποδεικτικά θα διατίθενται κατόπιν αιτήματος από τη Microsoft.</p>
15	<p>Όταν απαντά απευθείας στο Υποκείμενο δεδομένων ή όταν ο Προμηθευτής παρέχει έναν ηλεκτρονικό μηχανισμό αυτοεξυπηρέτησης, ο Προμηθευτής διαθέτει διεργασίες και διαδικασίες για ταυτοποίηση του Υποκειμένου δεδομένων που έχει στείλει το αίτημα.</p>	<p>Ο προμηθευτής έχει τεκμηριώσει τη μέθοδο που χρησιμοποιείται για ταυτοποίηση Υποκειμένων δεδομένων της Microsoft.</p> <p>Ο προμηθευτής θα παράσχει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
16	<p>Αν ζητηθεί από τη Microsoft να εντοπίσει Προσωπικά δεδομένα της Microsoft σχετικά με ένα Υποκείμενο δεδομένων τα οποία δεν είναι διαθέσιμα μέσω ηλεκτρονικού μηχανισμού αυτοεξυπηρέτησης, ο Προμηθευτής θα καταβάλλει εύλογες προσπάθειες εντοπισμού των δεδομένων που ζητούνται και θα τηρεί επαρκή αρχεία, ώστε να αποδεικνύει ότι πραγματοποιήθηκε εύλογη αναζήτηση.</p>	<p>Ο προμηθευτής θα διατηρεί τεκμηριωμένα αποδεικτικά ότι έχει ορίσει διαδικασίες για να διαπιστωθεί αν τηρούνται Προσωπικά δεδομένα της Microsoft και θα παράσχει τεκμηρίωση στη Microsoft κατόπιν αιτήματος.</p> <p>Ο προμηθευτής διατηρεί ένα αρχείο το οποίο επιδεικνύει τα μέτρα που λήφθηκαν για ικανοποίηση των αιτημάτων που αφορούν Δικαιώματα υποκειμένων δεδομένων.</p> <p>Η τεκμηρίωση περιλαμβάνει:</p> <ul style="list-style-type: none"> <li>▪ την ημερομηνία και την ώρα της αιτήματος,</li> <li>▪ τις ενέργειες που πραγματοποιήθηκαν ως προς το αίτημα και την καταγραφή του πότε ενημερώθηκε η Microsoft.</li> </ul> <p>Ο προμηθευτής θα παράσχει αποδεικτικά τήρησης αρχείων στη Microsoft κατόπιν αιτήματος.</p>

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα ΣΤ: Υποκείμενα δεδομένων (συνέχ.)</b>		
17	<p>Ο προμηθευτής θα ενημερώνει τα Υποκείμενα δεδομένων σχετικά με τα βήματα που πρέπει να ακολουθήσουν για να αποκτήσουν πρόσβαση στα Προσωπικά δεδομένα Microsoft που τους ανήκουν ή να ασκήσουν τα δικαιώματά τους αναφορικά με αυτά με οποιονδήποτε άλλο τρόπο.</p>	<p>Ο προμηθευτής θα διατηρεί τεκμηριωμένα αποδεικτικά της επικοινωνίας και των διαδικασιών για πρόσβαση στα Προσωπικά δεδομένα της Microsoft. Ο προμηθευτής θα διατηρεί τεκμηριωμένα αποδεικτικά και θα προσκομίσει αυτά τα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
18	<p>Να καταγράφεται η ημερομηνία και η ώρα των αιτημάτων που αφορούν Δικαιώματα Υποκειμένων δεδομένων και των ενεργειών που πραγματοποιεί ο προμηθευτής ως προς αυτά τα αιτήματα.</p> <p>Εάν απορριφθεί το αίτημα, κατόπιν οδηγιών της Microsoft, να παρέχει στο Υποκείμενο δεδομένων έγγραφη επεξήγηση.</p> <p>Να παρέχει αρχεία αιτημάτων Υποκειμένων δεδομένων στη Microsoft κατόπιν αιτήματος.</p>	<p>Ο προμηθευτής τηρεί αρχεία αιτημάτων για πρόσβαση και καταγράφει τις αλλαγές στα Προσωπικά δεδομένα της Microsoft.</p> <p>Να τεκμηριώνει τις περιπτώσεις απόρριψης αιτημάτων και να διατηρεί στοιχεία για έλεγχο και έγκριση από τη Microsoft.</p> <p>Ο προμηθευτής θα προσκομίζει αποδεικτικά τήρησης αρχείων των αιτημάτων και των απορρίψεων πρόσβασης στα Προσωπικά δεδομένα της Microsoft.</p>
19	<p>Ο προμηθευτής πρέπει να παρέχει τη δυνατότητα στη Microsoft ή να αποκτήσει ένα αντίγραφο των Προσωπικών δεδομένων της Microsoft που ζητούνται για το Υποκείμενο δεδομένων που έχει ολοκληρώσει τον έλεγχο ταυτότητας σε κατάλληλη έντυπη, ηλεκτρονική ή προφορική μορφή.</p>	<p>Ο προμηθευτής προμηθεύει Προσωπικά δεδομένα της Microsoft στο Υποκείμενο δεδομένων με τρόπο που είναι κατανοητός και με μορφή που εξυπηρετεί το Υποκείμενο δεδομένων και τον προμηθευτή.</p>
20	<p>Ο προμηθευτής πρέπει να λαμβάνει εύλογες προφυλάξεις, ώστε να διασφαλίζει ότι τα Προσωπικά δεδομένα της Microsoft που χορηγούνται στη Microsoft ή σε ένα Υποκείμενο δεδομένων που έχει ολοκληρώσει τον έλεγχο ταυτότητας δεν μπορούν να χρησιμοποιηθούν για την ταυτοποίηση κάποιου άλλου προσώπου.</p>	<p>Ο προμηθευτής θα διατηρεί τεκμηριωμένα αποδεικτικά των διαδικασιών που σχετίζονται με προφυλάξεις για αποφυγή της ταυτοποίησης του Υποκειμένου δεδομένων σε αντίθεση προς τους όρους της Σύμβασης. Ο προμηθευτής θα προσκομίζει αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
21	<p>Εάν το Υποκείμενο δεδομένων θεωρεί ότι τα Προσωπικά δεδομένα της Microsoft που του ανήκουν δεν είναι ολοκληρωμένα και ακριβή, ο προμηθευτής πρέπει να κλιμακώσει το ζήτημα στη Microsoft και να συνεργαστεί με τη Microsoft ανάλογα με τις ανάγκες, για την επίλυσή του.</p>	<p>Ο προμηθευτής τεκμηριώνει περιστατικά διαφωνίας και κλιμακώνει το ζήτημα στη Microsoft.</p> <p>Ο προμηθευτής θα προσκομίζει στη Microsoft τεκμηριωμένα αποδεικτικά κατόπιν αιτήματος.</p>



#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα Z: Υπεργολάβοι</b>		
	Εάν ο προμηθευτής σκοπεύει να χρησιμοποιήσει έναν υπεργολάβο για Επεξεργασία των Προσωπικών ή των Εμπιστευτικών δεδομένων της Microsoft, ο προμηθευτής πρέπει να κάνει τα εξής:	
22	<p>Να ειδοποιήσει τη Microsoft προτού αναθέσει υπηρεσίες υπεργολαβίας ή προβεί σε αλλαγές που αφορούν την προσθήκη ή την αντικατάσταση υπεργολάβων.</p> <p>Σημείωση: Υποδείξτε την από μέρους σας αποδοχή αυτής της υποχρέωσης, ακόμα και εάν επί του παρόντος δεν συνεργάζεστε με υπεργολάβους, αλλά ενδέχεται να το πράξετε στο μέλλον.</p>	Επικυρώστε ότι η Επεξεργασία των Προσωπικών δεδομένων της Microsoft πραγματοποιείται μόνο από εταιρείες τις οποίες γνωρίζει η Microsoft όπως απαιτείται στην ισχύουσα σύμβαση (π.χ. πρόταση εργασίας, προσάρτημα, εντολή αγοράς) ή καταγράφεται στη βάση δεδομένων SSPA. Ο Προμηθευτής μπορεί να δημοσιεύσει τη λίστα των υπεργολάβων του στο Διαδίκτυο και να συμπεριλάβει έναν σύνδεσμο προς τη σελίδα στη βάση δεδομένων SSPA.
23	Να τεκμηριώνει τη φύση και την έκταση των Προσωπικών και Εμπιστευτικών δεδομένων της Microsoft που υποβάλλονται σε δευτερεύουσα Επεξεργασία από υπεργολάβους, διασφαλίζοντας ότι οι πληροφορίες που συλλέγονται απαιτούνται για την Εκτέλεση καθηκόντων.	Ο προμηθευτής διατηρεί τεκμηρίωση σχετικά με τα Προσωπικά και Εμπιστευτικά δεδομένα της Microsoft που γνωστοποιούνται ή μεταβιβάζονται σε υπεργολάβους. Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.
24	Στην περίπτωση που η Microsoft είναι ένας Υπεύθυνος Επεξεργασίας Προσωπικών δεδομένων της Microsoft, να διασφαλίζει ότι ο υπεργολάβος χρησιμοποιεί τα Προσωπικά δεδομένα της Microsoft σύμφωνα με τις δηλωμένες προτιμήσεις επικοινωνίας του Υποκειμένου δεδομένων.	<p>Επιδείξτε τον τρόπο χρήσης μίας προτίμησης ενός Υποκειμένου δεδομένων της Microsoft από τους υπεργολάβους.</p> <p>Παράσχετε υποστηρικτική τεκμηρίωση (π.χ. στιγμιότυπο οθόνης, SLA, SOW κ.λπ.) που περιλαμβάνει το χρονικό πλαίσιο για εκπλήρωση μιας αλλαγής προτίμησης ενός υπεργολάβου.</p>
25	Να περιορίζει την Επεξεργασία προσωπικών δεδομένων της Microsoft από τον υπεργολάβο μόνο στον βαθμό που απαιτείται για εκπλήρωση της σύμβασης του προμηθευτή με τη Microsoft.	<p>Ο προμηθευτής μπορεί να παράσχει τεκμηρίωση που δείχνει ότι τα Προσωπικά δεδομένα της Microsoft που παρέχονται στον υπεργολάβο απαιτούνται για την Εκτέλεση καθηκόντων.</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
26	Να ελέγχει καταγγελίες για ενδείξεις μη εξουσιοδοτημένης ή Παράνομης επεξεργασίας προσωπικών δεδομένων της Microsoft.	<p>Ο προμηθευτής μπορεί να επιδείξει ότι υπάρχουν συστήματα και διαδικασίες για την αντιμετώπιση καταγγελιών σχετικά με μη εξουσιοδοτημένη χρήση ή γνωστοποίηση Προσωπικών δεδομένων της Microsoft από έναν υπεργολάβο.</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
---	---	-------------------------

## Ενότητα Z: Γνωστοποίηση σε τρίτα μέρη (συνέχ.)

27	Να ενημερώνει έγκαιρα τη Microsoft μόλις μαθαίνει ότι κάποιος υπεργολάβος διαθέτει Επεξεργασμένα προσωπικά ή εμπιστευτικά δεδομένα της Microsoft για οποιονδήποτε άλλο σκοπό εκτός από εκείνους που σχετίζονται με την Εκτέλεση καθηκόντων.	<p>Ο προμηθευτής έχει παράσχει την οδηγία και τα μέσα για να αναφέρει ένας υπεργολάβος την κατάχρηση δεδομένων της Microsoft.</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
28	Εάν ο προμηθευτής συλλέγει Προσωπικά δεδομένα από τρίτα μέρη για λογαριασμό της Microsoft, ο προμηθευτής πρέπει να επικυρώσει ότι οι πολιτικές και πρακτικές προστασίας δεδομένων τρίτων συνάδουν με τη σύμβαση του προμηθευτή με τη Microsoft και τις ΑΠΔ.	<p>Ο Προμηθευτής μπορεί να παράσχει τεκμηρίωση της δέουσας επιμέλειας που διενεργήθηκε σχετικά με τις πολιτικές και τις πρακτικές προστασίας δεδομένων τρίτων.</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
29	Να αναλαμβάνει έγκαιρα δράση για μετριασμό τυχόν πραγματικής ή δυνητικής βλάβης λόγω της μη εξουσιοδοτημένης ή Παράνομης Επεξεργασίας των Προσωπικών και Εμπιστευτικών δεδομένων της Microsoft από κάποιον υπεργολάβο.	<p>Ο προμηθευτής πρέπει να διατηρεί αποδεικτικά του σχεδίου και της διαδικασίας και να προσκομίζει αποδεικτικά τεκμηρίωση στη Microsoft κατόπιν αιτήματος.</p>

## Ενότητα Η: Ποιότητα

30	Ο προμηθευτής πρέπει να διατηρεί την ακεραιότητα όλων των Προσωπικών δεδομένων της Microsoft, διασφαλίζοντας ότι αυτά παραμένουν ακριβή, ολοκληρωμένα και συναφή με τους δηλωμένους σκοπούς για τους οποίους υποβλήθηκαν σε Επεξεργασία.	<p>Ο προμηθευτής μπορεί να επιδείξει ότι υπάρχουν διαδικασίες για επικύρωση Προσωπικών δεδομένων της Microsoft κατά τη συλλογή, τη δημιουργία και την ενημέρωσή τους.</p> <p>Ο προμηθευτής μπορεί να επιδείξει ότι υπάρχουν διαδικασίες εποπτείας και δειγματοληψίας για επαλήθευση της ακρίβειας σε συνεχή βάση, και διόρθωση, όταν χρειάζεται.</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
----	--	--

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα Θ: Παρακολούθηση και επιβολή</b>		
31	<p>Ο Προμηθευτής διαθέτει σχέδιο απόκρισης σε περιστατικά που απαιτεί ο Προμηθευτής να ειδοποιεί τη Microsoft χωρίς αδικαιολόγητη καθυστέρηση τη στιγμή που αντιλαμβάνεται ένα Περιστατικό παραβίασης δεδομένων.</p> <p>Ο προμηθευτής πρέπει, κατόπιν αιτήματος ή οδηγιών της Microsoft, να συνεργάζεται με τη Microsoft σε κάθε διερεύνηση, περιορισμό ή αποκατάσταση του Περιστατικού, συμπεριλαμβανομένης της παροχής στη Microsoft δεδομένων, πληροφοριών, πρόσβασης σε προσωπικό ή υλικό του Προμηθευτή που είναι απαραίτητο για διενέργεια μιας δικανικής εξέτασης.</p> <p>Σημείωση: Ανατρέξτε στον <a href="#">Οδηγό Προγράμματος SSPA</a> για τον τρόπο ειδοποίησης της Microsoft για ένα περιστατικό.</p>	<p>Ο προμηθευτής διαθέτει σχέδιο απόκρισης σε περιστατικά το οποίο περιλαμβάνει βήμα για ειδοποίηση των πελατών (της Microsoft) όπως περιγράφεται στην παρούσα ενότητα.</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
32	<p>Να υλοποιεί ένα σχέδιο αποκατάστασης και να παρακολουθεί την επίλυση κάθε Περιστατικού παραβίασης δεδομένων, ώστε να διασφαλίζεται η έγκαιρη κατάλληλη διορθωτική ενέργεια.</p>	<p>Ο προμηθευτής έχει τεκμηριώσει διαδικασίες στις οποίες θα προβεί για την απόκριση σε ένα Περιστατικό παραβίασης δεδομένων μέχρι το κλείσιμο.</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>
33	<p>Στην περίπτωση που η Microsoft είναι Υπεύθυνος Επεξεργασίας Προσωπικών δεδομένων της Microsoft, να θεσπίσει επίσημη διαδικασία καταγγελιών για απόκριση σε όλες τις καταγγελίες προστασίας δεδομένων που αφορούν Προσωπικά δεδομένα της Microsoft.</p>	<p>Ο προμηθευτής διαθέτει μέσα για λήψη καταγγελιών που αφορούν Προσωπικά δεδομένα της Microsoft και διαθέτει μια τεκμηριωμένη διαδικασία καταγγελιών για αντιμετώπιση καταγγελιών.</p> <p>Ο προμηθευτής θα προσκομίζει τεκμηριωμένα αποδεικτικά στη Microsoft κατόπιν αιτήματος.</p>

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα Ι: Ασφάλεια</b>		
	<p>Ο προμηθευτής πρέπει να θεσπίσει, να υλοποιήσει και να συντηρήσει ένα πρόγραμμα ασφάλειας πληροφοριών που περιλαμβάνει πολιτικές και διαδικασίες, ώστε τα Προσωπικά και Εμπιστευτικά δεδομένα της Microsoft να παραμένουν προστατευμένα και ασφαλή σύμφωνα με την καλή πρακτική του κλάδου και όπως απαιτείται από τη Νομοθεσία.</p> <p>Το πρόγραμμα ασφάλειας του προμηθευτή πρέπει να ανταποκρίνεται στα πρότυπα που καταγράφονται παρακάτω, στις απαιτήσεις 34-50.</p>	<p>Μια έγκυρη Πιστοποίηση ISO 27001 αποτελεί ένα αποδεκτό υποκατάστατο για την Ενότητα Ι. Επικοινωνήστε με το SSPA για την εφαρμογή αυτής της υποκατάστασης.</p> <p>Σημείωση: Θα χρειαστεί να παράσχετε την πιστοποίηση.</p>
34	<p>Να εκτελεί ετήσιες αξιολογήσεις ασφάλειας του δικτύου που περιλαμβάνουν:</p> <ul style="list-style-type: none"> <li>▪ έλεγχο σημαντικών αλλαγών στο περιβάλλον, όπως νέων στοιχείων συστήματος, τοπολογίας δικτύου, κανόνων τείχους προστασίας,</li> <li>▪ διεξαγωγή σαρώσεων ευπάθειας, και</li> <li>▪ τήρηση αρχείων καταγραφής αλλαγών.</li> </ul>	<p>Ο προμηθευτής διαθέτει τεκμηριωμένες αξιολογήσεις δικτύου, αρχεία καταγραφής αλλαγών και αποτελέσματα σάρωσης.</p> <p>Τα απαιτούμενα αρχεία καταγραφής αλλαγών πρέπει να παρακολουθούν τις αλλαγές, να παρέχουν πληροφορίες σχετικά με τον λόγο για την αλλαγή και να περιλαμβάνουν το όνομα και τον τίτλο του υπευθύνου έγκρισης.</p>
35	<p>Ο προμηθευτής πρέπει να ορίσει, να γνωστοποιήσει και να υλοποιήσει μια πολιτική κινητών συσκευών που διασφαλίζει και περιορίζει τη χρήση Προσωπικών ή Εμπιστευτικών δεδομένων της Microsoft στα οποία πραγματοποιείται πρόσβαση από κινητή συσκευή ή τα οποία χρησιμοποιούνται σε μια κινητή συσκευή.</p>	<p>Ο προμηθευτής επιδεικνύει χρήση μιας συμβατής πολιτικής κινητών συσκευών στις περιπτώσεις όπου η Επεξεργασία των Προσωπικών ή Εμπιστευτικών δεδομένων της Microsoft απαιτεί τη χρήση κινητής συσκευής.</p>
36	<p>Όλοι οι πόροι που χρησιμοποιούνται για την Εκτέλεση καθηκόντων πρέπει να έχουν υπολογιστεί και να έχουν προσδιορισμένο κάτοχο. Ο προμηθευτής φέρει την ευθύνη για τη συντήρηση μιας απογραφής αυτών των πόρων πληροφοριών, τη θέσπιση αποδεκτής και εξουσιοδοτημένης χρήσης των πόρων, καθώς και την εξασφάλιση κατάλληλου επιπέδου προστασίας για τους πόρους καθ' όλο τον κύκλο ζωής τους.</p>	<p>Απογραφή των πόρων συσκευών που χρησιμοποιούνται για την υποστήριξη της Εκτέλεσης καθηκόντων. Η απογραφή αυτών των πόρων πρέπει να περιλαμβάνει:</p> <ul style="list-style-type: none"> <li>▪ θέση συσκευής,</li> <li>▪ ταξινόμηση δεδομένων για τα δεδομένα στον πόρο,</li> <li>▪ αρχείο ανάκτησης πόρων κατά τη λήξη της απασχόλησης ή της επιχειρηματική σύμβασης, και</li> <li>▪ αρχείο απόρριψης μέσω αποθήκευσης δεδομένων, όταν δεν χρειάζονται πια.</li> </ul>

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα Ι: Ασφάλεια (συνέχ.)</b>		
37	<p>Θέσπιση και τήρηση διαδικασιών διαχείρισης δικαιωμάτων πρόσβασης, ώστε να αποτραπεί η μη εξουσιοδοτημένη πρόσβαση σε Προσωπικά ή Εμπιστευτικά δεδομένα της Microsoft που βρίσκονται υπό τον έλεγχο του προμηθευτή.</p>	<p>Ο προμηθευτής επιδεικνύει ότι έχει εφαρμόσει ένα σχέδιο διαχείρισης δικαιωμάτων πρόσβασης το οποίο περιλαμβάνει:</p> <ul style="list-style-type: none"> <li>▪ διαδικασίες ελέγχου πρόσβασης,</li> <li>▪ διαδικασίες ταυτοποίησης,</li> <li>▪ διαδικασίες κλειδώματος έπειτα από ανεπιτυχείς απόπειρες,</li> <li>▪ ισχυρές παραμέτρους για την επιλογή διαπιστευτηρίων ελέγχου ταυτότητας, και</li> <li>▪ απενεργοποίηση λογαριασμών χρηστών εντός 48 ωρών κατά τη λήξη της απασχόλησης,</li> <li>▪ ισχυρά στοιχεία ελέγχου κωδικού πρόσβασης που επιβάλλουν το μήκος και την πολυπλοκότητα του κωδικού πρόσβασης και αποτρέπουν την επαναχρησιμοποίηση.</li> </ul> <p>Ο προμηθευτής επιδεικνύει ότι διαθέτει καθιερωμένη διαδικασία για τον έλεγχο της πρόσβασης χρηστών σε Προσωπικά και Εμπιστευτικά δεδομένα της Microsoft, επιβάλλοντας την αρχή των ελάχιστων δυνατών προνομίων. Η διαδικασία περιλαμβάνει:</p> <ul style="list-style-type: none"> <li>▪ σαφώς προσδιορισμένους ρόλους χρηστών,</li> <li>▪ διαδικασίες για τον έλεγχο και την αιτιολόγηση της έγκρισης πρόσβασης σε ρόλους, και</li> <li>▪ δοκιμή ότι οι χρήστες με ρόλους που έχουν πρόσβαση σε δεδομένα της Microsoft διαθέτουν τεκμηριωμένη αιτιολόγηση για τη συμπερίληψή τους στην ομάδα/τον ρόλο.</li> </ul>
38	<p>Ορισμός και υλοποίηση διαδικασιών διαχείρισης ενημερωμένων εκδόσεων κώδικα που θέτουν σε προτεραιότητα τις ενημερώσεις κώδικα ασφαλείας για τα συστήματα που χρησιμοποιούνται για την Επεξεργασία των Προσωπικών ή των Εμπιστευτικών δεδομένων της Microsoft. Οι διαδικασίες αυτές περιλαμβάνουν τα εξής:</p> <ul style="list-style-type: none"> <li>▪ καθορισμένη προσέγγιση κινδύνου για τον ορισμό προτεραιοτήτων για ενημερωμένους κώδικες ασφαλείας</li> <li>▪ δυνατότητα χειρισμού και υλοποίησης ενημερωμένων κωδικών έκτακτης ανάγκης,</li> <li>▪ δυνατότητα εφαρμογής σε λειτουργικό σύστημα και λογισμικό διακομιστή, όπως σε διακομιστή εφαρμογών και λογισμικό βάσης δεδομένων,</li> <li>▪ τεκμηρίωση του κινδύνου που μετριάζεται με την ενημέρωση κώδικα και παρακολούθηση τυχόν εξαιρέσεων, και</li> <li>▪ απαιτήσεις για απόσυρση λογισμικού το οποίο δεν υποστηρίζεται πλέον από την εταιρεία σύνταξης.</li> </ul>	<p>Ο προμηθευτής μπορεί να επιδείξει μια υλοποιημένη διαδικασία διαχείρισης ενημερωμένου κώδικα που πληροί αυτήν την απαίτηση και καλύπτει, τουλάχιστον, τα ακόλουθα:</p> <ul style="list-style-type: none"> <li>▪ Αντιστοίχιση σοβαρότητας για την ενημέρωση της προτεραιότητας. (Οι ορισμοί σοβαρότητας τεκμηριώνονται.)</li> <li>▪ Τεκμηριωμένη διαδικασία για την υλοποίηση ενημερωμένου κώδικα έκτακτης ανάγκης.</li> <li>▪ Επικύρωση, ότι δεν γίνεται χρήση λειτουργικών συστημάτων τα οποία δεν υποστηρίζονται πλέον από την εταιρεία σύνταξης.</li> <li>▪ Αρχεία διαχείρισης ενημερώσεων κώδικα τα οποία παρακολουθούν εγκρίσεις και εξαιρέσεις.</li> </ul>

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα Ι: Ασφάλεια (συνέχ.)</b>		
39	<p>Εγκατάσταση προγράμματος προστασίας από ιούς και λογισμικό κακόβουλης λειτουργίας σε εξοπλισμό συνδεδεμένο με το δίκτυο ο οποίος χρησιμοποιείται για Επεξεργασία των Προσωπικών και των Εμπιστευτικών δεδομένων της Microsoft, συμπεριλαμβανομένων διακομιστών, υπολογιστών παραγωγής και εκπαίδευσης, για προστασία ενάντια στους δυνητικά επιβλαβείς ιούς και τις κακόβουλες εφαρμογές λογισμικού.</p> <p>Ενημέρωση των ορισμών του προγράμματος προστασίας από λογισμικό κακόβουλης λειτουργίας καθημερινά ή σύμφωνα με τις οδηγίες του προμηθευτή του προγράμματος προστασίας από ιούς/λογισμικό κακόβουλης λειτουργίας.</p> <p>Σημείωση: Αυτό ισχύει για όλα τα λειτουργικά συστήματα συμπεριλαμβανομένου του Linux.</p>	<p>Υπάρχουν αρχεία που δείχνουν ότι η χρήση λογισμικού προστασίας από ιούς και λογισμικό κακόβουλης λειτουργίας είναι ενεργή.</p> <p>Σημείωση: Αυτή η απαίτηση ισχύει για όλα τα λειτουργικά συστήματα.</p>
40	<p>Οι προμηθευτές που αναπτύσσουν λογισμικό για τη Microsoft πρέπει να ενσωματώσουν αρχές ασφάλειας βάσει σχεδιασμού στη διαδικασία δημιουργίας.</p>	<p>Τα έγγραφα τεχνικών προδιαγραφών του προμηθευτή περιλαμβάνουν σημεία ελέγχου για επικύρωση της ασφάλειας στους κύκλους ανάπτυξής τους.</p>
41	<p>Να εφαρμόζει πρόγραμμα Αποτροπής απώλειας δεδομένων («DLP») για αποτροπή εισβολών, απώλειας και άλλης μη εξουσιοδοτημένης δραστηριότητας. Τα δεδομένα πρέπει να είναι κατάλληλα ταξινομημένα, σημασμένα και προστατευμένα και ο προμηθευτής πρέπει να παρακολουθεί τα συστήματα πληροφοριών σε χρήση όπου γίνεται η Επεξεργασία των Προσωπικών ή Εμπιστευτικών δεδομένων της Microsoft, για εισβολές, απώλεια και άλλη μη εξουσιοδοτημένη δραστηριότητα.</p> <p>Το πρόγραμμα DLP, κατ' ελάχιστον:</p> <ul style="list-style-type: none"> <li>▪ απαιτεί χρήση πρότυπων Συστημάτων Εντοπισμού Εισβολών (Intrusion Detection System, «IDS») του κλάδου βάσει cloud, κεντρικού υπολογιστή και δικτύου, εάν διατηρείτε Προσωπικά ή Εμπιστευτικά δεδομένα της Microsoft,</li> <li>▪ απαιτεί υλοποίηση προηγμένων Συστημάτων Προστασίας Εισβολών (Intrusion Protection System, «IPS») διαμορφωμένα για την παρακολούθηση και ενεργή αποτροπή της απώλειας δεδομένων,</li> <li>▪ σε περίπτωση παραβίασης ενός συστήματος, απαιτεί ανάλυση του συστήματος, για να διασφαλιστεί η αντιμετώπιση τυχόν ευπαθειών που παραμένουν,</li> <li>▪ περιγράφει τις απαιτούμενες διαδικασίες για την παρακολούθηση εργαλείων εντοπισμού παραβίασης συστήματος,</li> <li>▪ καθορίζει μια διαδικασία απόκρισης και διαχείρισης περιστατικού που πρέπει να εκτελείται, όταν εντοπίζεται ένα Περιστατικό Παραβίασης δεδομένων, και</li> <li>▪ απαιτεί γνωστοποιήσεις (προς όλους τους υπαλλήλους και τους υπεργολάβους του προμηθευτή που καταργούνται από την Εκτέλεση του προμηθευτή) σχετικά με τη μη εξουσιοδοτημένη λήψη και χρήση Προσωπικών ή Εμπιστευτικών δεδομένων της Microsoft.</li> </ul>	<p>Τεκμηριωμένο πρόγραμμα DLP που έχει αναπτυχθεί με διαδικασίες για την αποτροπή εισβολών, απώλειας και άλλων μη εξουσιοδοτημένων δραστηριοτήτων (και, κατ' ελάχιστον, όλα τα στοιχεία που καθορίζονται σε αυτήν την ενότητα).</p>



#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα Ι: Ασφάλεια (συνέχ.)</b>		
42	Να ενημερώνει άμεσα τα ανώτερα διευθυντικά στελέχη και τη Microsoft σχετικά με τα αποτελέσματα της διερεύνησης από την απόκριση στο περιστατικό.	Πρέπει να υπάρχουν συστήματα και διαδικασίες για την ενημέρωση της Microsoft σχετικά με τα αποτελέσματα διερεύνησης απόκρισης σε περιστατικό.
43	Οι διαχειριστές συστήματος, το προσωπικό λειτουργιών, τα διευθυντικά στελέχη και οι τρίτοι πρέπει να υποβάλλονται σε ετήσια εκπαίδευση ασφάλειας.	Θέσπιση ενός εκπαιδευτικού προγράμματος ασφάλειας που περιλαμβάνει τα εξής: <ul style="list-style-type: none"> <li>▪ ετήσια εκπαίδευση για απόκριση σε περιστατικά, και</li> <li>▪ προσομοιωμένα συμβάντα και αυτοματοποιημένοι μηχανισμοί διευκόλυνσης μιας αποτελεσματικής απόκρισης σε καταστάσεις κρίσης.</li> <li>▪ Ευαισθητοποίηση σχετικά με την αποτροπή περιστατικών, όπως κινδύνων που σχετίζονται με τη λήψη κακόβουλου λογισμικού.</li> </ul>
44	Ο προμηθευτής πρέπει να διασφαλίσει ότι τα Προσωπικά και Εμπιστευτικά δεδομένα της Microsoft προστατεύονται με εφεδρικές διαδικασίες σχεδιασμού από τη μη εξουσιοδοτημένη χρήση, πρόσβαση, γνωστοποίηση, αλλοίωση και καταστροφή.	Ο προμηθευτής μπορεί να επιδείξει τεκμηριωμένες διαδικασίες απόκρισης και ανάκτησης οι οποίες περιγράφουν αναλυτικά τον τρόπο με τον οποίο θα διαχειριστεί ο οργανισμός ένα ενοχλητικό συμβάν και θα διατηρήσει την ασφάλεια πληροφοριών σε προκαθορισμένο επίπεδο βάσει εγκεκριμένων στόχων διαχείρισης για τη συνέχιση της ασφάλειας πληροφοριών. Ο προμηθευτής μπορεί να επιδείξει ότι έχει ορίσει και υλοποιήσει διαδικασίες για περιοδική δημιουργία αντιγράφων ασφαλείας, ασφαλή αποθήκευση και αποτελεσματική ανάκτηση κρίσιμων δεδομένων.
45	Να θεσπίζει και να δοκιμάζει σχέδια επιχειρησιακής συνέχειας και αποκατάστασης καταστροφής.	Το σχέδιο αποκατάστασης καταστροφής πρέπει να περιλαμβάνει τα εξής: <ul style="list-style-type: none"> <li>▪ Καθορισμένα κριτήρια για τον προσδιορισμό ενός συστήματος ως ζωτικής σημασίας για τη λειτουργία της επιχείρησης του προμηθευτή.</li> <li>▪ Αναφορά συστημάτων ζωτικής σημασίας με βάση τα καθορισμένα κριτήρια που πρέπει να τίθενται ως στόχος αποκατάστασης σε περίπτωση καταστροφής.</li> <li>▪ Ορισμένη διαδικασία αποκατάστασης καταστροφών για κάθε σύστημα ζωτικής σημασίας, η οποία διασφαλίζει ότι ένας μηχανικός που δεν γνωρίζει το σύστημα μπορεί να αποκαταστήσει την εφαρμογή εντός 72 ωρών.</li> <li>▪ Ετήσιες (ή συχνότερες) δοκιμές και έλεγχο των σχεδίων αποκατάστασης από καταστροφή, ώστε να διασφαλιστεί η ανταπόκριση στους στόχους αποκατάστασης.</li> </ul>

46	<p>Να ελέγχει την ταυτότητα ενός ατόμου προτού παραχωρήσει στο εν λόγω άτομο πρόσβαση σε Προσωπικά ή Εμπιστευτικά δεδομένα της Microsoft και να διασφαλίζει ότι η πρόσβαση περιορίζεται στο αντικείμενο δραστηριότητας του συγκεκριμένου ατόμου η οποία επιτρέπεται για την υποστήριξη της Εκτέλεσης.</p>	<p>Επιβεβαίωση ότι όλα τα αναγνωριστικά χρηστών είναι μοναδικά και ότι καθένα διαθέτει μέθοδο ελέγχου ταυτότητας που αποτελεί πρότυπο του κλάδου, όπως το <a href="#">Azure Active Directory</a>.</p> <p>Για πρόσβαση με αυξημένα δικαιώματα (διαχειριστικά προνόμια ή ενισχυμένα προνόμια άλλου τύπου) πρέπει να απαιτείται η χρήση δεύτερου παράγοντα, όπως προγράμματος ελέγχου ταυτότητας βάσει έξυπνης κάρτας ή τηλεφώνου.</p> <p>Τεκμηριωμένο πρόγραμμα ασφάλειας πληροφοριών που καλύπτει τη διαδικασία εξασφάλισης ότι η πρόσβαση όλων των υπαλλήλων και των υπεργολάβων του προμηθευτή σε Προσωπικά ή Εμπιστευτικά δεδομένα της Microsoft δεν υπερβαίνει σε εύρος ή διάρκεια την απαραίτητη για την υποστήριξη της Εκτέλεσης καθηκόντων.</p>
47	<p>Ο προμηθευτής πρέπει να προστατεύει όλα τα δεδομένα που υπόκεινται σε Επεξεργασία σε σχέση με την Εκτέλεση καθηκόντων και μετακινούνται μεταξύ δικτύων με κρυπτογράφηση, χρησιμοποιώντας το πρωτόκολλο Transport Layer Security («<a href="#">TLS</a>») ή Internet Protocol Security («<a href="#">IPsec</a>»).</p> <p>Αυτές οι μέθοδοι περιγράφονται στα NIST 800-52 και NIST 800-57. Μπορεί επίσης να χρησιμοποιηθεί αντίστοιχο πρότυπο του κλάδου.</p> <p>Ο προμηθευτής πρέπει να απορρίπτει την παροχή Προσωπικών ή Εμπιστευτικών δεδομένων της Microsoft που μεταβιβάζονται μέσω μη κρυπτογραφημένων μέσων.</p>	<p>Η διαδικασία δημιουργίας, ανάπτυξης και αντικατάστασης του TLS ή άλλων πιστοποιητικών πρέπει να είναι καθορισμένη και επιβεβλημένη.</p>
48	<p>Όλες οι συσκευές του προμηθευτή (φορητοί υπολογιστές, σταθμοί εργασίας κ.λπ.) που θα έχουν πρόσβαση σε Προσωπικά ή Εμπιστευτικά δεδομένα της Microsoft ή θα τα χειρίζονται πρέπει να χρησιμοποιούν κρυπτογράφηση βάσει δίσκου.</p>	<p>Κρυπτογραφήστε όλες τις συσκευές ώστε να ανταποκρίνονται στη λύση BitLocker ή σε κάποια άλλη αντίστοιχη λύση κρυπτογράφησης δίσκου του κλάδου για όλες τις συσκευές-πελάτες που χρησιμοποιούνται για χειρισμό Προσωπικών ή Εμπιστευτικών δεδομένων της Microsoft.</p>

#	Απαιτήσεις προστασίας δεδομένων προμηθευτών της Microsoft	Αποδεικτικά συμμόρφωσης
<b>Ενότητα I: Ασφάλεια (συνέχ.)</b>		
49	<p>Πρέπει να υπάρχουν συστήματα και διαδικασίες (τα οποία χρησιμοποιούν τρέχοντα πρότυπα του κλάδου, όπως αυτά που περιγράφονται στο πρότυπο <a href="#">NIST 800-111</a>) για κρυπτογράφηση σε κατάσταση αδράνειας (όταν είναι αποθηκευμένα) όλων των Προσωπικών ή/και Εμπιστευτικών δεδομένων της Microsoft, συμπεριλαμβανομένων όλων των εξής:</p> <ul style="list-style-type: none"> <li>▪ δεδομένα διαπιστευτηρίων (π.χ. όνομα χρήστη/κωδικούς πρόσβασης)</li> <li>▪ δεδομένα μεθόδου πληρωμής (π.χ. αριθμούς πιστωτικών καρτών και τραπεζικών λογαριασμών)</li> <li>▪ προσωπικά δεδομένα που αφορούν τη μετανάστευση</li> <li>▪ δεδομένα ιατρικού προφίλ (π.χ., αριθμούς ιατρικών φακέλων ή βιομετρικούς δείκτες ή αναγνωριστικά όπως DNA, δαχτυλικά αποτυπώματα, αμφιβληστροειδείς και ίριδες, φωνητικά μοτίβα, μοτίβα προσώπων και μετρήσεις χεριών που χρησιμοποιούνται για σκοπούς ελέγχου ταυτότητας)</li> <li>▪ δεδομένα αναγνώρισης που χορηγούνται από το κράτος (π.χ. αριθμοί κοινωνικής ασφάλισης ή άδειας οδήγησης)</li> <li>▪ δεδομένα που ανήκουν σε πελάτες της Microsoft (π.χ., SharePoint, έγγραφα O365, πελάτες OneDrive)</li> <li>▪ υλικό που αφορά προϊόντα της Microsoft τα οποία δεν έχουν ανακοινωθεί</li> <li>▪ Ημερομηνία γέννησης</li> <li>▪ Πληροφορίες προφίλ παιδιών</li> <li>▪ γεωγραφικά δεδομένα σε πραγματικό χρόνο</li> <li>▪ φυσική προσωπική (μη επαγγελματική) διεύθυνση</li> <li>▪ προσωπικό (μη επαγγελματικό) αριθμό τηλεφώνου</li> <li>▪ θρήσκευμα</li> <li>▪ πολιτικές απόψεις</li> <li>▪ σεξουαλικό προσανατολισμό/προτίμηση</li> <li>▪ απάντηση ερώτησης ασφαλείας (π.χ. έλεγχος ταυτότητας δύο παραγόντων, επαναφορά κωδικού πρόσβασης)</li> <li>▪ πατρώνυμο μητέρας</li> </ul>	<p>Ελέγξτε ότι τα Προσωπικά και Εμπιστευτικά δεδομένα της Microsoft σε αυτήν τη σειρά είναι κρυπτογραφημένα σε κατάσταση αδράνειας.</p>
50	<p>Ανωνυμοποιήστε όλα τα Προσωπικά δεδομένα της Microsoft που χρησιμοποιούνται σε περιβάλλον ανάπτυξης ή δοκιμών.</p>	<p>Τα Προσωπικά δεδομένα της Microsoft δεν πρέπει να χρησιμοποιούνται σε περιβάλλοντα ανάπτυξης ή δοκιμών. Εάν δεν υπάρχει εναλλακτική, πρέπει να ανωνυμοποιούνται επαρκώς, ώστε να αποτραπεί η αναγνώριση των Υποκειμένων δεδομένων ή η κατάχρηση Προσωπικών δεδομένων.</p> <p>Σημείωση: Τα ανωνυμοποιημένα δεδομένα διαφέρουν από τα ψευδωνυμοποιημένα δεδομένα. Τα ανωνυμοποιημένα δεδομένα είναι δεδομένα που δεν έχουν σχέση με ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο όπου το υποκείμενο των προσωπικών δεδομένων δεν είναι ή δεν είναι πλέον ταυτοποιήσιμο.</p>

**«Εξουσιοδοτημένος Αντιπρόσωπος»** είναι ένα άτομο που έχει το κατάλληλο επίπεδο εξουσιοδότησης να υπογράψει για λογαριασμό της εταιρείας. Αυτό το άτομο θα έχει τις απαραίτητες γνώσεις απορρήτου και ασφάλειας ή θα έχει συμβουλευτεί έναν ειδικό σε τέτοια θέματα προτού υποβάλει την απόκρισή του σε μια ενέργεια του Προγράμματος SSPA. Επιπλέον, προσθέτοντας το όνομά τους σε ένα έντυπο SSPA, πιστοποιούν ότι έχουν αναγνώσει και κατανοήσει τις ΑΠΔ.

**«EUDPR»** σημαίνει ο Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά όργανα, τους φορείς, τα γραφεία και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση του Κανονισμού (ΕΚ) υπ' αρ. 45/2001 και της απόφασης υπ' αρ. 1247/2002/ΕΚ.

Ως **«Ελεύθεροι επαγγελματίες»** νοούνται τα άτομα που εκτελούν εργασίες ή υπηρεσίες κατά παραγγελία, οι οποίες παρέχονται μέσω ψηφιακών πλατφορμών ή άλλων μέσων.

**«ΓΚΠΔ»** είναι ο Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της Οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία δεδομένων).

Ως **«Απαιτήσεις προστασίας προσωπικών δεδομένων»** σημαίνουν το ΓΚΠΔ, τους EUDPR, τους τοπικούς νόμους προστασίας δεδομένων ΕΕ/ΕΟΧ, το Νόμο περί Προστασίας Προσωπικών δεδομένων των Καταναλωτών της Καλιφόρνια, Αστικός Κώδικας της Καλιφόρνια § 1798.100 κ.επ. («CCPA»), τον Νόμο περί προστασίας δεδομένων του Ηνωμένου Βασιλείου του 2018 και τυχόν σχετικούς ή μεταγενέστερους νόμους, κανονισμούς και άλλες νομικές απαιτήσεις που ισχύουν στο ΗΒ, και τυχόν ισχύοντες νόμους, κανονισμούς και άλλες νομικές απαιτήσεις που σχετίζονται με (α) το απόρρητο και την ασφάλεια των δεδομένων, ή (β) τη χρήση, συλλογή, διατήρηση, αποθήκευση, ασφάλεια, αποκάλυψη, μετάδοση, απόρριψη και οποιαδήποτε άλλη επεξεργασία τυχόν Προσωπικών δεδομένων.

**«Πρότυπες ρήτρες ΕΕ» και «Τυπικές συμβατικές ρήτρες»** σημαίνουν (i) τις τυπικές ρήτρες προστασίας δεδομένων για μετάδοση προσωπικών δεδομένων σε υπεύθυνους επεξεργασίας που είναι εγκατεστημένοι σε τρίτες χώρες που δεν διασφαλίζουν ένα επαρκές επίπεδο προστασίας δεδομένων, όπως περιγράφεται στο άρθρο 46 του ΓΚΠΔ και που εγκρίθηκαν με την απόφαση (ΕΕ) 2021/914 της Ευρωπαϊκής Επιτροπής της 4ης Ιουνίου 2021· (ii) τυχόν διάδοχες τυπικές συμβατικές ρήτρες που έχουν υιοθετηθεί από (α) την Ευρωπαϊκή Επιτροπή, (β) τον Ευρωπαίο Επόπτη προστασίας δεδομένων και έχουν εγκριθεί από την Ευρωπαϊκή Επιτροπή, (γ) το Ηνωμένο Βασίλειο σύμφωνα με τον Γενικό Ομοσπονδιακό Νόμο για την Προστασία δεδομένων του Ηνωμένου Βασιλείου, (δ) Ελβετία σύμφωνα με τον Ελβετικό Ομοσπονδιακό Νόμο για την Προστασία δεδομένων, ή (ε) από κυβέρνηση σε δικαιοδοσία διαφορετική από την Ελβετία, το Ηνωμένο Βασίλειο και τις δικαιοδοσίες που περιλαμβάνουν την Ευρωπαϊκή Ένωση ή τον Ευρωπαϊκό Οικονομικό Χώρο όπου οι ρήτρες διέπουν τη διεθνή μετάδοση προσωπικών δεδομένων, θα ενσωματωθούν και θα δεσμευτούν για τον Προμηθευτή από την ημέρα της υιοθέτησής τους.

**«Φιλοξενία τοποθεσιών web»** Η υπηρεσία φιλοξενίας ιστοτόπων είναι μια διαδικτυακή υπηρεσία που δημιουργεί ή/και διατηρεί ιστοτόπους για λογαριασμό της Microsoft στον τομέα της Microsoft, δηλαδή, ο προμηθευτής παρέχει όλα τα υλικά και τις υπηρεσίες που απαιτούνται για τη δημιουργία και τη συντήρηση ενός ιστότοπου και τον καθιστά προσβάσιμο στο Διαδίκτυο. Ο «πάροχος υπηρεσιών φιλοξενίας ιστοτόπου» ή «πάροχος φιλοξενίας web» είναι ο προμηθευτής που παρέχει τα εργαλεία και τις υπηρεσίες που απαιτούνται για προβολή του ιστότοπου ή της ιστοσελίδας στο Διαδίκτυο, όπως cookie ή ιστοφάρους για διαφημίσεις.