ΕΚΘΕΣΗ ΑΞΙΟΛΟΓΗΣΗΣ ΣΥΜΜΟΡΦΩΣΗΣ ΤΩΝ ΛΟΓΙΣΜΙΚΩΝ ΤΗΣ MICROSOFT ΜΕ ΤΟΝ ΓΚΠΔ

Οικονομικό Πανεπιστήμιο Αθηνών

1/7/2025

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΚΘΕΣΗ ΑΞΙΟΛΟΓΗΣΗΣ ΣΥΜΜΟΡΦΩΣΗΣ ΤΩΝ ΛΟΓΙΣΜΙΚΩΝ ΤΗΣ MICROSOFT ΜΕ ΤΟΝ ΓΚΠΔ

Η Διεύθυνση Ψηφιακής Διακυβέρνησης του Οικονομικού Πανεπιστημίου Αθηνών στο πλαίσιο του Ψηφιακού Ανασχηματισμού προχωρά σε αναβάθμιση της υπηρεσίας Email του Πανεπιστημίου ώστε να ανταποκρίνεται στις τρέχουσες συνθήκες του ακαδημαϊκού χώρου, καθώς και στις ανάγκες προστασίας και ασφάλειας της υπηρεσίας σύμφωνα με την τρέχουσα Πολιτική του Πανεπιστημίου.

Ο Σκοπός της Έκθεσης

Η σύνταξη της έκθεσής αυτής έχει ως σκοπό, να εξετάσει το κατά πόσο το σύστημα διαχείρισης επικοινωνίας της Microsoft (Microsoft Exchange – υπηρεσία Email) είναι συμμορφωμένο με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ.

Βασικοί όροι του ΓΚΠΔ

Ο ΓΚΠΔ θέτει 26 ορισμούς για να οριοθετήσει το πλαίσιο της προστασίας των δεδομένων προσωπικού χαρακτήρα. Οι πιο σημαντικοί από αυτούς είναι:

«Δεδομένα προσωπικού χαρακτήρα» αποτελεί κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου.

«Επεξεργασία» είναι κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή.

«Υπεύθυνος επεξεργασίας» είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο Υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους.

«Εκτελών την επεξεργασία» είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας.

«Αποδέκτης» είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας, στα οποία κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, είτε πρόκειται για τρίτον είτε όχι. Ωστόσο οι Δημόσιες αρχές που ενδέχεται να λάβουν δεδομένα προσωπικού χαρακτήρα στο πλαίσιο συγκεκριμένης έρευνας σύμφωνα με το δίκαιο της Ένωσης ή κράτους μέλους δεν θεωρούνται ως αποδέκτες· η επεξεργασία των δεδομένων αυτών από τις εν λόγω δημόσιες αρχές πραγματοποιείται σύμφωνα με τους ισχύοντες κανόνες προστασίας των δεδομένων ανάλογα με τους σκοπούς της επεξεργασίας.

«Τρίτος» θεωρείται οποιοδήποτε φυσικό ή νομικό πρόσωπο, δημόσια αρχή, υπηρεσία ή φορέας, με εξαίρεση το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας, τον εκτελούντα την επεξεργασία και τα πρόσωπα τα οποία, υπό την άμεση εποπτεία του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία, είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα,

«Παραβίαση δεδομένων προσωπικού χαρακτήρα» είναι η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.

Νομοθετικό πλαίσιο συμμόρφωσης

Το πλαίσιο ορίζεται από:

- τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ) ΕΕ679/2016 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ,
- τον Ν.4624/2019 που αποτυπώνει τα μέτρα εφαρμογής του Κανονισμού (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 ενσωματώνει στην εθνική νομοθεσία την Οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και

- τις κατευθυντήριες οδηγίες του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων καθώς και τις οδηγίες της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ).

Συμμόρφωση της Microsoft με τον ΓΚΠΔ

Η Microsoft είναι μια εταιρεία που απευθύνεται σε μεγάλους παγκόσμιους οργανισμούς και επιχειρήσεις, σε διάφορα εκπαιδευτικά Ιδρύματα ανά την Υφήλιο καθώς και σε δημόσιους φορείς και Αρχές κρατών.

Σε ότι αφορά τα προσωπικά δεδομένα η Microsoft έχει αναρτημένο DPA (Data Processing Agreement-έκδοσης του Απριλίου του 2025) ως Παράρτημα Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στο οποίο καθορίζονται υποχρεώσεις προστασίας προσωπικών δεδομένων και με το οποίο όλοι όσοι συμβάλλονται μαζί της συμφωνούν. Το παράρτημα ενσωματώνεται δι' αναφοράς στους όρους Προϊόντων και σε άλλες συμβάσεις της Microsoft. Το παράρτημα συνοδεύει την συγκεκριμένη έκθεση (Συν_1) αλλά είναι προσβάσιμο και στο Link:

https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA?lang=15&year=2025

Με το συγκεκριμένο παράρτημα η Microsoft αποδέχεται ρόλο εκτελούντος την Επεξεργασία και επεξεργάζεται τα δεδομένα σύμφωνα με τις οδηγίες που έχουν δοθεί από τον Υπεύθυνο Επεξεργασίας. Στην περίπτωση της σύμβασης του Πανεπιστημίου για την παροχή της email Υπηρεσίας, ως Υπεύθυνος Επεξεργασίας θεωρείται το Οικονομικό Πανεπιστήμιο Αθηνών.

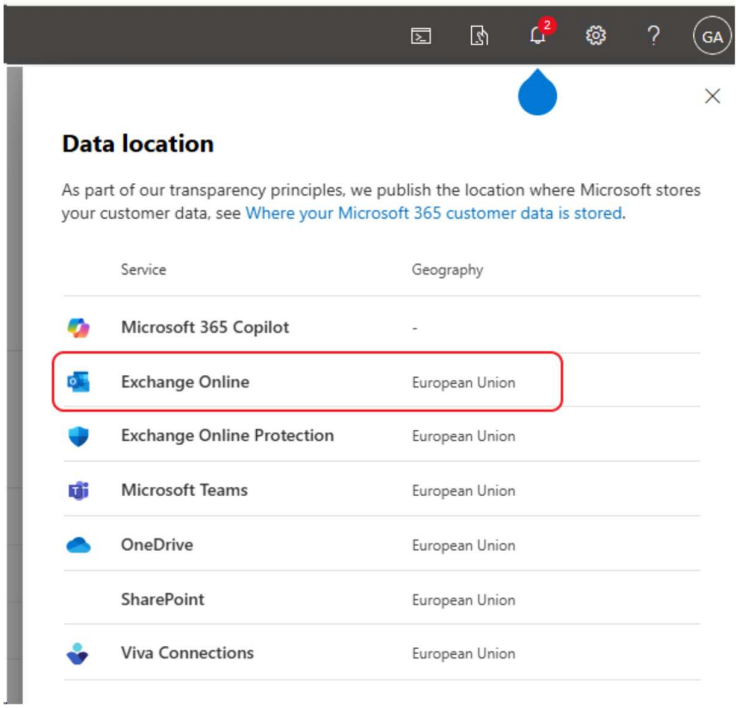
Παρόλο που το συγκεκριμένο DPA έχει συνταχθεί για να καλύπτει και άλλους Κανονισμούς Προστασίας Δεδομένων εκτός της Ευρωπαϊκής Ένωσης, σε πολλά σημεία αναφέρεται ρητώς και στον ΓΚΠΔ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

Στο παράρτημα αυτό υπάρχει εκτεταμένο Παράρτημα που αφορά στα Μέτρα Ασφάλειας (παράρτημα Α), Πρόσθετα Μέτρα ασφάλειας (Παράρτημα Γ) και Συνημμένο αναφορικά με τους όρους του Γενικού Κανονισμού για την Προστασία Δεδομένων της Ευρωπαϊκής Ένωσης (συμβατό με τις απαιτήσεις του ΓΚΠΔ).

Τοποθεσία επεξεργασίας και Διαβιβάσεις

Η Microsoft φροντίζει η επεξεργασία δεδομένων να πραγματοποιείται εντός του Ευρωπαϊκού Χώρου ώστε να είναι συμβατή με τους όρους του ΓΚΠΔ. Ιδιαίτερα όμως για την email Υπηρεσία, όπως αναφέρεται και στην έκθεση του προϊσταμένου της

Διεύθυνσης Ψηφιακής Διακυβέρνησης, η τοποθεσία αποθήκευσης των δεδομένων είναι η Ευρωπαϊκή Ένωση.



Παρόλα αυτά η Microsoft όπως αναφέρεται στο Έγγραφό της: Compliance with EU transfer requirements for personal data in the Microsoft Cloud (Συν_2) ακολουθώντας τις συστάσεις του Ευρωπαϊκού Συμβουλίου για την Προστασία Δεδομένων παίρνει πρόσθετα μέτρα και για τα δεδομένα που προέρχονται από την Ευρωπαϊκή Ένωση και επεξεργάζονται σε χώρες εκτός αυτής, ενισχύοντας την διαφάνεια, τις διαδικασίες μεταφοράς αλλά και των συνθηκών επεξεργασίας στις τρίτες χώρες.

Για τον λόγο αυτό η Microsoft έχει διαθέσιμα εργαλεία αναζήτησης και καθορισμού της τοποθεσίας που είναι αποθηκευμένα τα δεδομένα, ώστε ακόμη και αν χρειάζεται (για άλλες υπηρεσίες) να μεταφέρει δεδομένα σε Τρίτες χώρες, τότε αυτό πραγματοποιείται με υψηλό επίπεδο ασφάλειας.

Β. Τεχνικά Μέτρα

Η Microsoft υποστηρίζει κρυπτογράφηση και μάλιστα σε όλα τα επίπεδα. Οπότε αναφέρεται δυνατότητα κρυπτογράφησης (encryption) in transit, at rest και in use. Εκτός από την κρυπτογράφηση των δεδομένων που υποστηρίζει και η οποία αποτελεί προτεινόμενο τεχνικό μέτρο, το οποίο αναφέρεται ρητώς στον ΓΚΠΔ, υιοθετεί και άλλα τεχνικά μέτρα. Διαθέτει σύστημα διαχείρισης πόρων με απογραφή πόρων, περιορισμό πρόσβασης (φυσική και ψηφιακή) σε αυτούς. Έχει εργαλεία DLP (Data Loss Prevention), και διαδικασίες ανάκτησης δεδομένων. Διαθέτει λογισμικά ελέγχου λογισμικών κακόβουλης λειτουργίας.

Η Microsoft δίνει στον πελάτη της την δυνατότητα να έχει πρόσβαση στα πληροφοριακά συστήματά της, που περιέχουν δεδομένα του και τηρεί αρχεία καταγραφής πρόσβασης (log files), έχει ισχυρά ελεγχόμενο σύστημα πρόσβασης στα δεδομένα (authentication και authorization), με μεγάλη ιεράρχηση ρόλων δικαιωμάτων πρόσβασης.

Β. Οργανωτικά Μέτρα - Πιστοποιήσεις

Ταυτόχρονα η Microsoft ως εκτελών την Επεξεργασία παρέχει επαρκείς εγγυήσεις από πλευράς εμπειρογνωσίας, αξιοπιστίας και πόρων που ανταποκρίνονται στις απαιτήσεις του ΓΚΠΔ.

Η Microsoft εφαρμόζει ισχυρά οργανωτικά μέτρα για την προστασία των δεδομένων, συμπεριλαμβανομένης της οργάνωσης της ασφάλειας των πληροφοριών, της διαχείρισης περιουσιακών στοιχείων, της ασφάλειας ανθρώπινων πόρων, της φυσικής και περιβαλλοντικής ασφάλειας, της διαχείρισης λειτουργιών, του ελέγχου πρόσβασης, της διαχείρισης συμβάντων ασφαλείας και της διαχείρισης της επιχειρηματικής συνέχειας. Τα μέτρα αυτά ορίζονται στην Πολιτική Ασφαλείας της Microsoft και πληρούν τα καθιερωμένα πρότυπα του κλάδου για την ασφάλεια δεδομένων, όπως αυτά καθορίζονται από διεθνή πρότυπα όπως τα ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27018, και ISO/IEC 27701.

Να σημειώσω εδώ ότι το ISO/IEC 27001 είναι το διεθνές πρότυπο «Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικότητας» που εκδόθηκε στις 25.10.2022 και αντικαθιστά το ISO/IEC 27001:2013. Το συγκεκριμένο πρότυπο ελλείψει άλλου ευρωπαϊκού προτύπου συγκεντρώνει εν πολλοίς τις απαιτήσεις του ΓΚΠΔ.

Το ISO/IEC 27002 αφορά την «Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία ιδιωτικότητας - Έλεγχοι προστασίας πληροφοριών»

Το ISO/IEC 27018 αφορά «Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κώδικας πρακτικής για προστασία PII σε δημόσια υπολογιστικά νέφη που λειτουργούν ως επεξεργαστές PII» και είναι χρήσιμο εχέγγυο για τους οργανισμούς που προσφέρουν cloud υπηρεσίες.

Το και ISO/IEC 27701 αποτελεί επέκταση των ISO 27001 και ISO 27002 κυρίως ως προς τις τεχνικές ασφάλειας - για τη διαχείριση πληροφοριών απορρήτου , τις απαιτήσεις και οδηγίες.

Η Microsoft διαθέτει επίσης και την πιστοποίηση ISO/IEC 42001:2023 η οποία θέτει τις απαιτήσεις για τη δημιουργία, την εφαρμογή, τη διατήρηση και τη συνεχή βελτίωση ενός συστήματος διαχείρισης Τεχνητής Νοημοσύνης (ΤΝ).

Περισσότερες πληροφορίες σχετικά με τις πιστοποιήσεις της Microsoft βρίσκονται και στο Link: https://servicetrust.microsoft.com/viewpage/ISOIEC και στο Συν_3_ISO Report της Microsoft