Microsoft Procurement

Οδηγός του προγράμματος SSPA (Διασφάλιση απορρήτου και ασφάλειας προμηθευτών)

Έκδοση 8

Ιούνιος 2022

Εισαγωγή

Στη Microsoft, πιστεύουμε ότι η προστασία του απορρήτου αποτελεί θεμελιώδες δικαίωμα. Στην αποστολή μας να ενισχύσουμε κάθε άτομο και οργανισμό στον πλανήτη ώστε να επιτύχουν περισσότερα, προσπαθούμε να κερδίζουμε και να διατηρούμε την εμπιστοσύνη των πελατών μας κάθε ημέρα.

Οι ισχυρές πρακτικές απορρήτου και ασφάλειας είναι πολύ σημαντικές για την αποστολή μας, θεμελιώδεις για την εμπιστοσύνη των πελατών, και σε πολλές δικαιοδοσίες απαιτούνται από τη νομοθεσία. Τα πρότυπα που αποτυπώνονται στις πολιτικές απορρήτου και ασφάλειας της Microsoft αντικατοπτρίζουν τις αξίες μας ως εταιρείας και ισχύουν επίσης για τους προμηθευτές μας (όπως η εταιρεία σας) που επεξεργάζονται δεδομένα Microsoft εκ μέρους της Microsoft.

Το Πρόγραμμα διασφάλισης απορρήτου και ασφάλειας προμηθευτών («**SSPA**») είναι το εταιρικό πρόγραμμα της Microsoft που παρέχει στους προμηθευτές μας βασικές οδηγίες επεξεργασίας των δεδομένων Microsoft, μέσω των Απαιτήσεων προστασίας δεδομένων («**DPR**») προμηθευτών της Microsoft, που διατίθενται στο SSPA στη διεύθυνση Microsoft.com/Procurement. Σημειώστε ότι οι προμηθευτές ενδέχεται να πρέπει να πληρούν πρόσθετες απαιτήσεις οργανωτικού επιπέδου που αποφασίζονται και κοινοποιούνται εκτός του SSPA από τον όμιλο της Microsoft που είναι υπεύθυνος για την επικοινωνία με τον εκάστοτε προμηθευτή.

Οι βασικοί όροι SSPA ορίζονται στο DPR. Για να μάθετε περισσότερα σχετικά με το πρόγραμμα, διαβάστε τις Συχνές ερωτήσεις και επικοινωνήστε με την παγκόσμια ομάδα μας στη διεύθυνση SSPAHelp@microsoft.com.

Επισκόπηση του προγράμματος SSPA

Το SSPA είναι μια κοινοπραξία μεταξύ των τμημάτων Microsoft Procurement, Corporate External and Legal Affairs, και Corporate Security, ώστε να διασφαλιστεί ότι οι αρχές απορρήτου και ασφάλειας τηρούνται από τους προμηθευτές μας.

Η εμβέλεια του SSPA καλύπτει όλους τους προμηθευτές παγκοσμίως που επεξεργάζονται Προσωπικά δεδομένα και/ή Εμπιστευτικά δεδομένα της Microsoft τα οποία σχετίζονται με την εκτέλεση καθηκόντων του εκάστοτε 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**»).

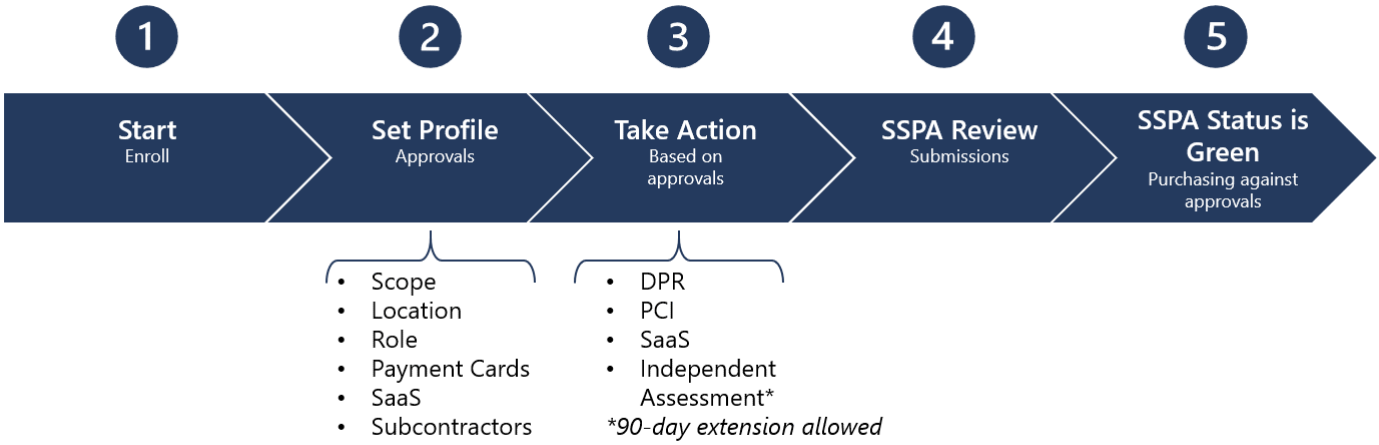
Το SSPA δίνει τη δυνατότητα στον προμηθευτή να κάνει επιλογές Προφίλ επεξεργασίας δεδομένων που ευθυγραμμίζονται με τα αγαθά και/ή τις υπηρεσίες για τις οποίες έχετε συνάψει σύμβαση να παρέχετε (βάσει της Εκτέλεσης καθηκόντων σας). Αυτές οι επιλογές ενεργοποιούν αντίστοιχες απαιτήσεις για παροχή διασφαλίσεων συμμόρφωσης στη Microsoft.

Όλοι οι εγγεγραμμένοι προμηθευτές πρέπει να ολοκληρώσουν μια αυτοβεβαίωση συμμόρφωσης με το DPR ετησίως. Το Προφίλ επεξεργασίας δεδομένων σας προσδιορίζει αν

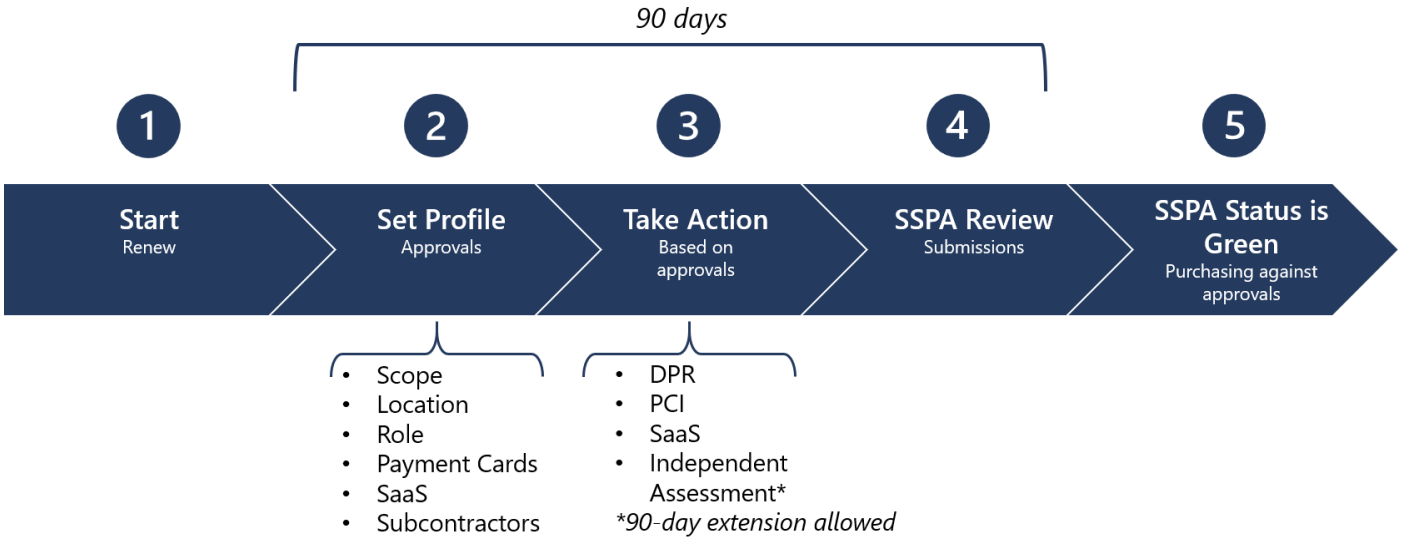
πρέπει να εκδοθεί το πλήρες DPR ή αν ισχύει ένα υποσύνολο απαιτήσεων. Οι προμηθευτές που επεξεργάζονται δεδομένα τα οποία η Microsoft θεωρεί ότι ενέχουν υψηλότερο κίνδυνο ενδέχεται επίσης να χρειαστεί να πληρούν πρόσθετες απαιτήσεις, όπως η παροχή ανεξάρτητης επαλήθευσης της συμμόρφωσης. Οι προμηθευτές που βρίσκονται σε δημοσιευμένη λίστα Υπεργολάβων επεξεργασίας της Microsoft θα κληθούν επίσης να παράσχουν ανεξάρτητη επαλήθευση της συμμόρφωσης.

Σημαντικό: Οι δραστηριότητες συμμόρφωσης προσδιορίζουν μια κατάσταση SSPA: Πράσινο (συμμόρφωση) ή Κόκκινο (μη συμμόρφωση). Τα εργαλεία αγορών της Microsoft επικυρώνουν ότι η κατάσταση SSPA είναι Πράσινο (για κάθε προμηθευτή στην εμβέλεια του SSPA) προτού επιτραπεί σε μια δέσμευση να προχωρήσει.

Διάγραμμα διαδικασίας SSPA – Εγγραφή νέου προμηθευτή



Διάγραμμα διαδικασίας SSPA – Ετήσια ανανέωση προμηθευτή



Εμβέλεια SSPA

Για να προσδιορίσετε αν εσείς (ο προμηθευτής) επεξεργάζεστε Προσωπικά δεδομένα και/ή Εμπιστευτικά δεδομένα της Microsoft, δείτε τη λίστα παραδειγμάτων στους παρακάτω πίνακες. Λάβετε υπόψη σας ότι πρόκειται για παραδείγματα και όχι για εξαντλητική λίστα.
Σημείωση: Ένας ιδιοκτήτης επιχείρησης Microsoft μπορεί να ζητήσει εγγραφή εκτός της συγκεκριμένης λίστας, αν πρέπει να ληφθεί υπόψη ο εμπιστευτικός χαρακτήρας των δεδομένων υπό επεξεργασία.

Προσωπικά δεδομένα ανά τύπο δεδομένων

Τα παραδείγματα περιλαμβάνουν ενδεικτικά, μεταξύ άλλων:

Ευαίσθητα δεδομένα
Δεδομένα που σχετίζονται με παιδιά
Γενετικά δεδομένα, βιομετρικά δεδομένα ή δεδομένα υγείας
Φυλετική ή εθνοτική καταγωγή
Πολιτικές, θρησκευτικές ή φιλοσοφικές πεποιθήσεις, απόψεις και διασυνδέσεις
Συνδρομή μέλους σε συνδικαλιστική οργάνωση
Σεξουαλική ζωή ή σεξουαλικός προσανατολισμός ενός φυσικού προσώπου
Μεταναστευτική κατηγορία (βίζα, άδεια εργασίας κ.λπ.)
Κρατικά αναγνωριστικά στοιχεία (διαβατήριο, άδεια οδήγησης, βίζα, αριθμοί κοινωνικής ασφάλισης, αριθμοί εθνικής ταυτότητας)
Ακριβή δεδομένα τοποθεσίας χρήστη (εντός 300 μέτρων)
Αριθμοί προσωπικών τραπεζικών λογαριασμών
Αριθμός και ημερομηνία λήξης πιστωτικής κάρτας
Δεδομένα περιεχομένου πελάτη
Έγγραφα, φωτογραφίες, βίντεο, μουσική κ.λπ.
Κριτικές και/ή αξιολογήσεις που έχουν εισαχθεί σε ένα προϊόν ή μια υπηρεσία
Απαντήσεις σε έρευνες
Ιστορικό, ενδιαφέροντα και αγαπημένα περιήγησης
Γραφή, πληκτρολόγηση και εκφωνήματα (ομιλία/ήχος και/ή συνομιλία/bot)
Δεδομένα διαπιστευτηρίων (κωδικοί πρόσβασης, υποδείξεις κωδικών πρόσβασης, όνομα χρήστη, βιομετρικά δεδομένα που χρησιμοποιούνται για ταυτοποίηση)
Δεδομένα πελατών που είναι συσχετισμένα με μια υπόθεση υποστήριξης

Καταγεγραμμένα και παραγόμενα δεδομένα
Δεδομένα μη ακριβούς τοποθεσίας
Διεύθυνση IP
Προτιμήσεις και εξατομίκευση συσκευής
Χρήση υπηρεσιών για ιστότοπους, ανίχνευση των κλικ σε ιστοσελίδες
Δεδομένα μέσων κοινωνικής δικτύωσης, σχέσεις κοινωνικού διαγράμματος
Δεδομένα δραστηριότητας από συνδεδεμένες συσκευές, όπως συσκευές καταγραφής φυσικής κατάστασης
Στοιχεία επικοινωνίας, όπως όνομα, διεύθυνση, αριθμός τηλεφώνου, διεύθυνση email, ημερομηνία γέννησης, εξαρτώμενες επαφές και επαφές έκτακτης ανάγκης
Αξιολόγηση απάτης και κινδύνων, έλεγχος ιστορικού
Στοιχεία ασφάλισης, σύνταξης, επιδομάτων
Βιογραφικά υποψήφιων, σημειώσεις/σχόλια συνεντεύξεων
Metadata and telemetry
Δεδομένα Λογαριασμού
Δεδομένα οργάνων πληρωμής
Αριθμός και ημερομηνία λήξης πιστωτικής κάρτας
Στοιχεία δρομολόγησης τραπεζών
Αριθμός τραπεζικού λογαριασμού
Αιτήματα πίστωσης ή πιστωτικού ορίου
Φορολογικά έγγραφα και αναγνωριστικά
Δεδομένα επενδύσεων ή εξόδων
Εταιρικές κάρτες
Ψευδωνυμοποιημένα στοιχεία τελικού χρήστη (EUPI) (αναγνωριστικά που δημιουργούνται από τη Microsoft για αναγνώριση των χρηστών προϊόντων και υπηρεσιών της Microsoft)
Καθολικά μοναδικό αναγνωριστικό (GUID)
Αναγνωριστικό ή μοναδικό αναγνωριστικό χρήστη Passport (PUID)
Κατακερματισμένα ταυτοποιήσιμα στοιχεία τελικού χρήστη (EUII)
Αναγνωριστικά συνεδριών
Αναγνωριστικά συσκευών
Διαγνωστικά δεδομένα

Δεδομένα καταγραφών
Online Customer Data
Microsoft online enterprise customer (example: Azure tenant, M365 tenant…)
Microsoft consumer customer (example: Xbox Live, OneDrive Consumer, …)
Microsoft enterprise customer (on premises customer)
Support data (example: Customer originates a ticket)
Account data (example: billing data, e-commerce)
Survey/Event Registration/Training

Εμπιστευτικά δεδομένα της Microsoft ανά κατηγορία δεδομένων

Τα παραδείγματα περιλαμβάνουν ενδεικτικά, μεταξύ άλλων:

Αυστηρά εμπιστευτικό
Πληροφορίες που αφορούν ή σχετίζονται με την ανάπτυξη, τη δοκιμή ή την κατασκευή των Προϊόντων Microsoft ή των εξαρτημάτων των Προϊόντων Microsoft *Το λογισμικό, οι διαδικτυακές υπηρεσίες ή το υλισμικό της Microsoft που πωλείται εμπορικά σε οποιοδήποτε κανάλι θεωρείται «**Προϊόν Microsoft**»*
Πληροφορίες μάρκετινγκ προκυκλοφορίας για συσκευές Microsoft
Μη δημοσιευμένα εταιρικά οικονομικά δεδομένα της Microsoft που υπόκεινται στους κανόνες SEC
Εμπιστευτικό
Κλειδιά αδειών χρήσης προϊόντων της Microsoft εκ μέρους της Microsoft για διανομή μέσω οποιασδήποτε μεθόδου
Πληροφορίες που αφορούν ή σχετίζονται με την ανάπτυξη ή τη δοκιμή εσωτερικών εφαρμογών Επιχειρηματικής δραστηριότητας (Line of Business - LOB) της Microsoft
Υλικό μάρκετινγκ προκυκλοφορίας της Microsoft για λογισμικό και υπηρεσίες Microsoft, όπως Office, SQL, Azure κ.λπ.
Γραπτή, σχεδιαστική, ηλεκτρονική ή έντυπη τεκμηρίωση για οποιεσδήποτε υπηρεσίες ή προϊόντα της Microsoft, όπως συσκευές (οδηγοί βημάτων ή διαδικασιών, δεδομένα ρύθμισης παραμέτρων, κ.λπ.)

Σημαντικό: Ένας κάτοχος επιχείρησης Microsoft μπορεί να απαιτήσει συμμετοχή για δεδομένα που δεν περιλαμβάνονται σε αυτήν τη λίστα.

Προφίλ επεξεργασίας δεδομένων

Οι προμηθευτές Microsoft έχουν τον έλεγχο ως προς το Προφίλ επεξεργασίας δεδομένων SSPA τους.

Αυτό επιτρέπει στους προμηθευτές να αποφασίζουν ποιες δεσμεύσεις θέλουν να εκτελούν (βάσει της Εκτέλεσης καθηκόντων). Δώστε ιδιαίτερη προσοχή στις επιλογές και λάβετε υπόψη σας τη δραστηριότητα συμμόρφωσης που πρέπει να ολοκληρωθεί για να επιτύχετε την έγκριση. **Ανατρέξτε στην ενότητα «Απαιτήσεις διασφάλισης» παρακάτω και στο Παράρτημα Α**.

Οι επιχειρηματικοί όμιλοι της Microsoft θα μπορούν να δημιουργούν δεσμεύσεις με προμηθευτές μόνο όταν η δραστηριότητα επεξεργασίας δεδομένων αντιστοιχεί στις εγκρίσεις που έχει λάβει ο εκάστοτε προμηθευτής.

Οι προμηθευτές θα μπορούν να ενημερώσουν το Προφίλ επεξεργασίας δεδομένων τους ανά πάσα στιγμή κατά τη διάρκεια του έτους, **αν δεν υπάρχουν ανοιχτές εργασίες**. Αν πραγματοποιηθεί κάποια αλλαγή, θα εκδοθεί η αντίστοιχη δραστηριότητα και πρέπει να ολοκληρωθεί πριν από την εξασφάλιση των εγκρίσεων. Οι υπάρχουσες, ολοκληρωμένες εγκρίσεις θα ισχύουν μέχρι να ολοκληρωθούν οι νέες απαιτήσεις.

Αν οι εργασίες που εκτελέστηκαν πρόσφατα δεν ολοκληρωθούν εντός του επιτρεπόμενου χρονικού πλαισίου των 90 ημερών, η κατάσταση SSPA θα αλλάξει σε Κόκκινο (μη συμμόρφωση) και ο λογαριασμός ενδέχεται να απενεργοποιηθεί από τα συστήματα Πληρωτέων λογαριασμών της Microsoft.

Εγκρίσεις επεξεργασίας δεδομένων	
1	Εμβέλεια επεξεργασίας δεδομένων ▪ Εμπιστευτικό ▪ Προσωπικό, Εμπιστευτικό
2	Τοποθεσία επεξεργασίας δεδομένων ▪ Στη Microsoft ή στον Πελάτη ▪ Στον Προμηθευτή
3	Ρόλος επεξεργασίας δεδομένων ▪ Υπεύθυνος επεξεργασίας (Ανεξάρτητος ή Από κοινού) ▪ Εργολάβος επεξεργασίας ▪ Υπεργολάβος επεξεργασίας (που έχει οριστεί από τη Microsoft)
4	Επεξεργασία καρτών πληρωμής ▪ Ναι ▪ Δεν εφαρμόζεται
5	Λογισμικό ως υπηρεσία ▪ Ναι ▪ Δεν εφαρμόζεται
6	Χρήση υπεργολάβων ▪ Ναι ▪ Δεν εφαρμόζεται

Θέματα έγκρισης

Εμβέλεια επεξεργασίας δεδομένων

Εμπιστευτικό

Επιλέξτε αυτήν την έγκριση αν η Εκτέλεση καθηκόντων του προμηθευτή θα περιλαμβάνει την επεξεργασία μόνο Εμπιστευτικών δεδομένων της Microsoft.

Αν επιλέξετε αυτήν την έγκριση, δεν θα πληροίτε τις προϋποθέσεις για δεσμεύσεις επεξεργασίας Προσωπικών δεδομένων.

Προσωπικό, Εμπιστευτικό

Επιλέξτε αυτήν την έγκριση αν η Εκτέλεση καθηκόντων του προμηθευτή θα περιλαμβάνει την επεξεργασία Προσωπικών και Εμπιστευτικών δεδομένων της Microsoft.

Τοποθεσία επεξεργασίας

Στη Microsoft ή στον Πελάτη

Επιλέξτε αυτήν την έγκριση αν η Απόδοση του προμηθευτή περιλαμβάνει την επεξεργασία δεδομένων από τον προμηθευτή εντός του περιβάλλοντος δικτύου της Microsoft, όπου το προσωπικό χρησιμοποιεί τα διαπιστευτήρια πρόσβασης *@microsoft.com* ή εντός του περιβάλλοντος ενός πελάτη της Microsoft.

Μην επιλέξετε αυτήν την επιλογή υπό αυτές τις περιστάσεις:

- Ο Προμηθευτής διαχειρίζεται μια υπεράκτια εγκατάσταση που έχει οριστεί από τη Microsoft.
- Ο Προμηθευτής παρέχει πόρους στη Microsoft και κατά καιρούς εργάζεται εντός και εκτός του δικτύου της Microsoft. Η τοποθεσία επεξεργασίας για εργασία εκτός δικτύου θεωρείται «στον προμηθευτή».

Στον Προμηθευτή
Αν δεν ισχύει η συνθήκη «Στη Microsoft ή στον Πελάτη» (όπως περιγράφεται παραπάνω), επιλέξτε αυτήν τη ρύθμιση.

_____

Ρόλος επεξεργασίας δεδομένων

Υπεύθυνος επεξεργασίας (καλύπτει τους ανεξάρτητους και τους από κοινού υπεύθυνους επεξεργασίας)

Επιλέξτε αυτήν την έγκριση αν **όλες** οι πτυχές της Εκτέλεσης καθηκόντων του προμηθευτή πληρούν τον ορισμό του ρόλου επεξεργασίας δεδομένων «Υπεύθυνος επεξεργασίας» (δείτε το DPR).

Αν επιλέξετε αυτήν την έγκριση, δεν θα πληροίτε τις προϋποθέσεις για επεξεργασία Προσωπικών δεδομένων με τον ρόλο «Εργολάβος επεξεργασίας». Αν ένας προμηθευτής είναι ταυτόχρονα Εργολάβος επεξεργασίας και Υπεύθυνος επεξεργασίας της Microsoft, επιλέξτε «Εργολάβος επεξεργασίας», όχι «Υπεύθυνος επεξεργασίας».

Εργολάβος επεξεργασίας

Αυτός είναι ο πιο κοινός ρόλος επεξεργασίας όταν οι προμηθευτές επεξεργάζονται δεδομένα εκ μέρους της Microsoft. Ανατρέξτε στον ορισμό του Εργολάβου επεξεργασίας στο DPR.

Υπεργολάβος επεξεργασίας

Ο Υπεργολάβος επεξεργασίας είναι ένα τρίτο μέρος το οποίο η Microsoft δεσμεύει για Εκτέλεση καθηκόντων, όπου η Εκτέλεση καθηκόντων περιλαμβάνει Επεξεργασία προσωπικών δεδομένων της Microsoft για τα οποία η Microsoft είναι Υπεύθυνος επεξεργασίας. Οι προμηθευτές δεν μπορούν να αυτοπροσδιοριστούν ως Υπεργολάβοι επεξεργασίας στη Microsoft, διότι απαιτείται προέγκριση από εσωτερικές ομάδες Απορρήτου. Ένας προμηθευτής μπορεί να είναι Υπεργολάβος επεξεργασίας μόνο όταν η Microsoft είναι ο Εργολάβος επεξεργασίας δεδομένων, και ο

προμηθευτής επεξεργάζεται Τύπους προσωπικών δεδομένων επιχειρήσεων που πληρούν τα κριτήρια. Οι Υπεργολάβοι επεξεργασίας θα έχουν πρόσθετες απαιτήσεις σύμβασης και συμμόρφωσης, συμπεριλαμβανομένων ενός Παραρτήματος προστασίας δεδομένων και μιας Ανεξάρτητης αξιολόγησης (δείτε παρακάτω).

Επεξεργασία καρτών πληρωμής

Επιλέξτε αυτήν την έγκριση αν οποιοδήποτε μέρος των δεδομένων που επεξεργάζεται ο προμηθευτής περιλαμβάνει δεδομένα για υποστήριξη επεξεργασίας πιστωτικών καρτών ή άλλων καρτών πληρωμής εκ μέρους της Microsoft.

Αυτή η έγκριση επιτρέπει σε έναν προμηθευτή να συμμετέχει σε δεσμεύσεις επεξεργασίας καρτών πληρωμής.

_____

Λογισμικό

Το τμήμα Microsoft Procurement κατευθύνει τους αγοραστές μέσω μιας διαδικασίας εισαγωγής για όλες τις αγορές λογισμικού. Αυτό περιλαμβάνει διάφορους ελέγχους, συμπεριλαμβανομένης της διαλογής SSPA, για να αποφασιστεί αν ο προμηθευτής που παρέχει το λογισμικό είναι εντός της εμβέλειας για τη διαχείριση SSPA. (Οι Αγοραστές της Microsoft μπορούν να ανατρέξουν στα βήματα που περιγράφονται στην εσωτερική σελίδα Λογισμικό και υπηρεσία cloud ProcureWeb για περισσότερες λεπτομέρειες). Αν απαιτείται το SSPA, οι προμηθευτές ενδέχεται επίσης να χρειαστεί να προσδιορίσουν ότι ισχύει η επιλογή προφίλ «Λογισμικό ως υπηρεσία» (SaaS). Για τους εγγεγραμμένους προμηθευτές SSPA, αυτό μπορεί να γίνει κατά την ολοκλήρωση του Προφίλ επεξεργασίας δεδομένων στην Πύλη συμμόρφωσης προμηθευτών της Microsoft.

Για σκοπούς συμμόρφωσης με το SSPA, αντιμετωπίστε το SaaS ευρέως για να συμπεριλάβετε επίσης την Πλατφόρμα ως υπηρεσία (PaaS) και την Υποδομή ως υπηρεσία (IaaS). (Για περισσότερες πληροφορίες σχετικά με το SaaS, ανατρέξτε σε αυτήν την επεξήγηση.)

Λογισμικό ως υπηρεσία (SaaS)

Το Λογισμικό ως υπηρεσία (SaaS) επιτρέπει στους χρήστες να συνδέονται και να χρησιμοποιούν ιστοπαγείς εφαρμογές στο Διαδίκτυο.

Η Microsoft ορίζει το **Λογισμικό ως υπηρεσία (SaaS)** ως λογισμικό το οποίο βασίζεται σε κοινό κώδικα που χρησιμοποιείται σε ένα μοντέλο ένα-σε-πολλά σε βάση πληρωμής ανάλογα με τη χρήση ή ως συνδρομή που βασίζεται σε μετρήσεις χρήσης. Ο πάροχος υπηρεσιών cloud αναπτύσσει και διατηρεί ιστοπαγές λογισμικό, παρέχει αυτόματες ενημερώσεις λογισμικού και καθιστά λογισμικό διαθέσιμο στους πελάτες του μέσω Διαδικτύου σε βάση ένα-σε-πολλά ή πληρωμής ανάλογα με τη χρήση. Αυτή η μέθοδος παράδοσης και αδειοδότησης λογισμικού επιτρέπει την πρόσβαση στο λογισμικό διαδικτυακά μέσω συνδρομής, και όχι μέσω αγοράς και εγκατάστασης σε κάθε μεμονωμένο υπολογιστή.

Σημείωση: Οι περισσότεροι προμηθευτές SaaS θα πρέπει να προσθέσουν την έγκριση Υπεργολάβου στην Πύλη συμμόρφωσης προμηθευτών της Microsoft, αν τα

Προσωπικά δεδομένα ή τα Εμπιστευτικά δεδομένα της Microsoft φιλοξενούνται σε πλατφόρμα τρίτου μέρους.

Χρήση υπεργολάβων

Επιλέξτε αυτήν την έγκριση αν ο προμηθευτής συνεργάζεται με Υπεργολάβους για την Εκτέλεση καθηκόντων (ανατρέξτε στο DPR για τους ορισμούς).

Συμπεριλαμβάνονται επίσης οι ελεύθεροι επαγγελματίες (δείτε το ΔΚΔ).

Απαιτήσεις διασφάλισης

Απαιτήσεις βάσει εγκρίσεων προφίλ

Οι εγκρίσεις που έχουν επιλεγεί στο Προφίλ επεξεργασίας δεδομένων σας βοηθούν το SSPA στην αξιολόγηση του επιπέδου κινδύνου για όλες τις δεσμεύσεις σας ως προς τη Microsoft. Οι απαιτήσεις συμμόρφωσης του SSPA διαφέρουν βάσει του Προφίλ επεξεργασίας δεδομένων και των συσχετισμένων εγκρίσεων. Η ενότητα αυτή εξηγεί τις διάφορες απαιτήσεις SSPA.

Υπάρχουν επίσης συνδυασμοί που ενδέχεται να αυξήσουν ή να μειώσουν τις απαιτήσεις συμμόρφωσης. Οι συνδυασμοί αποτυπώνονται στο Παράρτημα Α και εκεί θα βρείτε αυτά που αναμένεται να εκτελέσετε από την Πύλη συμμόρφωσης προμηθευτών της Microsoft μετά την ολοκλήρωση του προφίλ σας. Μπορείτε ανά πάσα στιγμή να επικυρώσετε τον τρόπο με τον οποίο η δική σας περίπτωση αντιστοιχεί σε αυτό το πλαίσιο, ζητώντας έλεγχο από την ομάδα SSPA.

Ενέργεια: Βρείτε το προφίλ έγκρισής σας στο Παράρτημα Α και ελέγξτε τις αντίστοιχες απαιτήσεις διασφάλισης και τις επιλογές Ανεξάρτητης διασφάλισης, αν ισχύουν.

Σημαντικό: Αν το προφίλ σας περιλαμβάνει Λογισμικό ως υπηρεσία (SaaS), Υπεργολάβους, φιλοξενία ιστότοπων ή κάρτες πληρωμής, απαιτείται πρόσθετη διασφάλιση.

Αυτοβεβαίωση για το DPR

Όλοι οι προμηθευτές που είναι εγγεγραμμένοι στο SSPA πρέπει να ολοκληρώσουν μια αυτοβεβαίωση συμμόρφωσης προς το DPR εντός 90 ημερών από την παραλαβή του αιτήματος. Αυτό το αίτημα παρέχεται σε ετήσια βάση, αλλά μπορεί να είναι πιο συχνό αν το Προφίλ επεξεργασίας δεδομένων ενημερωθεί στα μέσα του έτους. Οι λογαριασμοί προμηθευτών θα αλλάξουν στην κατάσταση SSPA «Κόκκινο» (μη συμμόρφωση) σε περίπτωση υπέρβασης της περιόδου των 90 ημερών. Η επεξεργασία νέων εντολών αγοράς εντός της εμβέλειας θα είναι δυνατή μόνο αφού η κατάσταση SSPA αλλάξει σε «Πράσινο» (συμμόρφωση).

Οι νεοεγγεγραμμένοι προμηθευτές πρέπει να ολοκληρώσουν τις απαιτήσεις που έχουν εκδοθεί ώστε να λάβουν την Πράσινη (συμμόρφωση) κατάσταση SSPA πριν από την έναρξη των δεσμεύσεων.

Σημαντικό: Η ομάδα SSPA δεν είναι εξουσιοδοτημένη να παρέχει επεκτάσεις για αυτήν την εργασία.

Οι Εξουσιοδοτημένοι αντιπρόσωποι που θα ολοκληρώσουν την αυτοβεβαίωση θα πρέπει να διασφαλίσουν ότι διαθέτουν επαρκείς πληροφορίες από εμπειρογνώμονες επί του θέματος για να απαντήσουν σε κάθε απαίτηση με σιγουριά. Επιπλέον, αν προσθέσουν το όνομά τους σε μια φόρμα έντυπο SSPA, πιστοποιούν ότι έχουν αναγνώσει και κατανοήσει το DPR. Οι προμηθευτές μπορούν να προσθέσουν άλλες επαφές στο διαδικτυακό εργαλείο για να βοηθήσουν στην ολοκλήρωση των απαιτήσεων.

Ο Εξουσιοδοτημένος αντιπρόσωπος (δείτε τον ορισμό στο DPR) κάνει τις εξής ενέργειες:

1. Προσδιορίζει ποιες απαιτήσεις ισχύουν.
2. Αναρτά μια απάντηση για κάθε ισχύουσα απαίτηση.
3. Υπογράφει και υποβάλλει τη βεβαίωση στην Πύλη συμμόρφωσης προμηθευτών της Microsoft.

Εφαρμοσιμότητα

Οι προμηθευτές αναμένεται να ανταποκριθούν σε όλες τις ισχύουσες απαιτήσεις DPR που έχουν εκδοθεί σύμφωνα με το Προφίλ επεξεργασίας δεδομένων. Αναμένεται ότι, στο πλαίσιο των εκδομένων απαιτήσεων, κάποιες απαιτήσεις ενδέχεται να μην ισχύουν για τα προϊόντα ή τις υπηρεσίες που παρέχει ο προμηθευτής στη Microsoft. Αυτές οι απαιτήσεις μπορούν να σημανθούν ως «δεν ισχύει» με ένα λεπτομερές σχόλιο για επικύρωση από τους ελεγκτές SSPA.

Οι υποβολές DPR ελέγχονται από την ομάδα SSPA για τυχόν επιλογές «δεν ισχύει», «τοπική νομική διένεξη» ή «συμβατική διένεξη» έναντι των εκδομένων απαιτήσεων. Η ομάδα SSPA ενδέχεται να ζητήσει διευκρινίσεις για μία ή περισσότερες επιλογές. Οι τοπικές νομικές και συμβατικές διενέξεις γίνονται αποδεκτές μόνο αν παρέχονται υποστηρικτικές παραπομπές και η διένεξη είναι σαφής.

Απαίτηση ανεξάρτητης αξιολόγησης

Ανατρέξτε στις Απαιτήσεις βάσει εγκρίσεων στο Παράρτημα Α για να δείτε τις εγκρίσεις επεξεργασίας δεδομένων που ενεργοποιούν αυτήν την απαίτηση.

Οι προμηθευτές έχουν την επιλογή να αλλάξουν τις εγκρίσεις ενημερώνοντας το Προφίλ επεξεργασίας δεδομένων τους. Ωστόσο, αν ο προμηθευτής έχει τον Ρόλο επεξεργασίας δεδομένων «Υπεργολάβος επεξεργασίας», ο προμηθευτής δεν θα μπορεί να αλλάξει αυτήν την έγκριση και θα απαιτείται να διενεργεί Ανεξάρτητη αξιολόγηση σε ετήσια βάση.

Για να εξασφαλίσουν τις εγκρίσεις που απαιτούν ανεξάρτητη επαλήθευση της συμμόρφωσης, οι προμηθευτές θα πρέπει να επιλέξουν έναν ανεξάρτητο αξιολογητή για επικύρωση της συμμόρφωσης με το DPR. Ο αξιολογητής πρέπει να προετοιμάσει μια συμβουλευτική επιστολή για παροχή διασφαλίσεων συμμόρφωσης στη Microsoft. Η παρούσα επιστολή πρέπει να είναι ανεπιφύλακτη και όλα τα ζητήματα μη συμμόρφωσης πρέπει να επιλυθούν και να αποκατασταθούν πριν από την υποβολή της επιστολής επιβεβαίωσης στην Πύλη συμμόρφωσης προμηθευτών της Microsoft για εξέταση από την ομάδα SSPA. Οι αξιολογητές μπορούν να πραγματοποιήσουν λήψη ενός εγκεκριμένου προτύπου συμβουλευτικής επιστολής, το οποίο είναι συνημμένο στο PDF «Προτιμώμενοι αξιολογητές» που διατίθεται εδώ.

Το **Παράρτημα Α** περιλαμβάνει αποδεκτές εναλλακτικές λύσεις πιστοποίησης, αν επιλέξετε να μη χρησιμοποιήσετε ανεξάρτητο αξιολογητή για επαλήθευση της συμμόρφωσης με το DPR (κατά περίπτωση, όπως για προμηθευτές SaaS, προμηθευτές φιλοξενίας ιστότοπων ή προμηθευτές με Υπεργολάβους). Το ISO 27701 (προστασία απορρήτου) και το ISO 27001 (ασφάλεια) θεωρείται ότι παρέχουν στενή αντιστοίχιση με το DPR.

Όταν ο Προμηθευτής είναι πάροχος υπηρεσιών υγείας στις Ηνωμένες Πολιτείες ή καλυπτόμενη οντότητα, θα αποδεχτούμε μια έκθεση HITRUST όσον αφορά την κάλυψη απορρήτου και ασφάλειας.

Το SSPA ενδέχεται να διενεργήσει ανεξάρτητη αξιολόγηση χειροκίνητα, αν προκύψουν περιστάσεις πέραν των συνήθων που απαιτούν πρόσθετες διαδικασίες δέουσας επιμέλειας. Κάποια παραδείγματα είναι: αίτημα απορρήτου ή ασφάλειας τμήματος, επικύρωση αποκατάστασης περιστατικού δεδομένων, ή απαίτηση για αυτοματοποιημένη εκτέλεση δικαιωμάτων υποκειμένου δεδομένων.

Οδηγίες για προσέγγιση αυτής της απαίτησης:

1. Η δέσμευση πρέπει να πραγματοποιηθεί από έναν αξιολογητή με επαρκή τεχνική κατάρτιση και γνώσεις για επαρκή αξιολόγηση της συμμόρφωσης.
2. Οι αξιολογητές πρέπει να είναι μέλη της Διεθνούς Ομοσπονδίας Λογιστών (IFAC) ή του Αμερικανικού Ινστιτούτου Ορκωτών Ελεγκτών Λογιστών (AICPA), ή να διαθέτουν πιστοποιήσεις από άλλους σχετικούς οργανισμούς απορρήτου και ασφάλειας, όπως η Διεθνής Ένωση Επαγγελματιών Απορρήτου (IAPP) ή η Ένωση Παρακολούθησης και Ελέγχου Πληροφοριακών Συστημάτων (ISACA).
3. Ο αξιολογητής πρέπει να χρησιμοποιεί το πλέον πρόσφατο DPR που περιλαμβάνει τα αποδεικτικά που απαιτούνται για υποστήριξη κάθε απαίτησης. **Οι προμηθευτές θα πρέπει να παρέχουν στον αξιολογητή απαντήσεις βάσει της πιο πρόσφατα εγκεκριμένης βεβαίωσης DPR που διαθέτουν.**
4. Σε περίπτωση νεοεγγεγραμμένου προμηθευτή, ο αξιολογητής θα ελέγξει τον σχεδιασμό των στοιχείων ελέγχου διαδικασίας. Σε όλες τις άλλες περιπτώσεις, ο αξιολογητής θα ελέγξει την αποτελεσματικότητα των στοιχείων ελέγχου.
5. Η εμβέλεια της δέσμευσης αξιολόγησης ισχύει μόνο για τα Προσωπικά δεδομένα και/ή τα Εμπιστευτικά δεδομένα της Microsoft σε σχέση με την Εκτέλεση καθηκόντων του εν λόγω προμηθευτή.
6. Η εμβέλεια της δέσμευσης αξιολόγησης ισχύει μόνο για όλες τις δραστηριότητες επεξεργασίας δεδομένων εντός της εμβέλειας που εκτελούνται έναντι του αριθμού λογαριασμού προμηθευτή που έλαβε το αίτημα. Αν ο προμηθευτής επιλέξει ταυτόχρονα περισσότερους από έναν λογαριασμούς προμηθευτή, η **επιστολή βεβαίωσης πρέπει να περιλαμβάνει τη λίστα λογαριασμών προμηθευτή που περιλαμβάνονται στην αξιολόγηση και τις συσχετισμένες διευθύνσεις.**
7. Η επιστολή που υποβάλλεται στο SSPA δεν πρέπει να περιλαμβάνει δηλώσεις για τις οποίες ο προμηθευτής δεν μπορεί να εκπληρώσει τις Απαιτήσεις προστασίας δεδομένων όπως έχουν συνταχθεί. Αυτά τα ζητήματα πρέπει να διορθωθούν πριν από την υποβολή της επιστολής.

Το SSPA έχει καταστήσει διαθέσιμη μια λίστα προτιμώμενων αξιολογητών. Αυτές οι εταιρείες είναι εξοικειωμένες με τη διεξαγωγή αξιολογήσεων SSPA. Οι προμηθευτές αναμένεται να καλύψουν το κόστος της εν λόγω αξιολόγησης, το οποίο ποικίλλει ανάλογα με την κλίμακα και την εμβέλεια της επεξεργασίας δεδομένων.

Απαίτηση πιστοποίησης PCI DSS

Το Πρότυπο ασφάλειας δεδομένων κλάδου καρτών πληρωμής (PCI DSS) είναι ένα πλαίσιο για ανάπτυξη ισχυρής ασφάλειας δεδομένων καρτών πληρωμής που περιλαμβάνει την πρόληψη, την ανίχνευση και την κατάλληλη αντίδραση σε περιστατικά ασφάλειας. Το πλαίσιο αναπτύχθηκε από το Συμβούλιο Προτύπων Ασφάλειας PCI, έναν αυτορρυθμιζόμενο οργανισμό του κλάδου. Ο σκοπός των απαιτήσεων PCI DSS είναι ο εντοπισμός ευπαθών σημείων στην τεχνολογία και στις διαδικασίες που θέτουν σε κίνδυνο την ασφάλεια των δεδομένων κατόχων καρτών που υποβάλλονται σε επεξεργασία.

Η Microsoft υποχρεούται να συμμορφώνεται με αυτά τα πρότυπα. Αν ένας προμηθευτής χειρίζεται στοιχεία καρτών πληρωμής εκ μέρους της Microsoft, απαιτείται αποδεικτικό της τήρησης αυτών των προτύπων. Επισκεφθείτε το Συμβούλιο Προτύπων Ασφάλειας PCI για να κατανοήσετε τις απαιτήσεις που έχουν οριστεί από τον οργανισμό PCI.

Ανάλογα με τον όγκο των συναλλαγών υπό επεξεργασία, ο προμηθευτής θα πρέπει να ζητήσει από έναν Καταρτισμένο αξιολογητή ασφάλειας να πιστοποιήσει τη συμμόρφωση, ή μπορεί να συμπληρώσει ένα έντυπο ερωτηματολόγιο αυτοαξιολόγησης.

Οι επωνυμίες καρτών πληρωμής ορίζουν τα όρια για τον τύπο αξιολόγησης, σε γενικές γραμμές έχουν ως εξής:

- Επίπεδο 1: Παροχή πιστοποιητικού PCI AOC αξιολογητή τρίτου μέρους
- Επίπεδο 2 ή 3: Παροχή ενός Ερωτηματολογίου αυτοαξιολόγησης PCI DSS (SAQ) που έχει υπογραφεί από το στέλεχος του προμηθευτή.

Υποβολή της πιστοποίησης που ισχύει και πληροί τις απαιτήσεις PCI.

Απαίτηση για Λογισμικό ως υπηρεσία

Οι προμηθευτές που πληρούν τον ορισμό SaaS που περιλαμβάνεται στο Προφίλ επεξεργασίας δεδομένων ενδέχεται να απαιτείται να παράσχουν έγκυρη πιστοποίηση ISO 27001, αν αυτό απαιτείται από τη Συμφωνία υπηρεσιών cloud της Microsoft.

Οι ελεγκτές SSPA θα επικυρώσουν ότι η υποβολή σας πληροί τη συμβατική υποχρέωση.

Μην υποβάλετε πιστοποίηση κέντρου δεδομένων. Αναμένουμε την πιστοποίηση ISO 27001 που ισχύει για τις υπηρεσίες λογισμικού που αναγράφονται στη σύμβασή σας με τη Microsoft.

Χρήση υπεργολάβων

Η Microsoft θεωρεί ότι η χρήση υπεργολάβων αποτελεί παράγοντα υψηλού κινδύνου. Οι προμηθευτές που χρησιμοποιούν υπεργολάβους οι οποίοι θα επεξεργαστούν Προσωπικά και/ή Εμπιστευτικά δεδομένα της Microsoft πρέπει να γνωστοποιήσουν αυτούς τους

υπεργολάβους. Επιπλέον, ο προμηθευτής θα πρέπει επίσης να γνωστοποιήσει τις χώρες στις οποίες τα εν λόγω προσωπικά δεδομένα θα υποβληθούν σε επεξεργασία από κάθε υπεργολάβο.

Περιστατικά δεδομένων

Αν ένας προμηθευτής αντιληφθεί ένα περιστατικό δεδομένων απορρήτου ή ασφάλειας, πρέπει να ενημερώσει τη Microsoft όπως περιγράφεται λεπτομερώς και ορίζεται στο DPR.

Αναφορά περιστατικού δεδομένων μέσω του SupplierWeb ή μέσω email στη διεύθυνση SupplR @microsoft.com

Φροντίστε να συμπεριλάβετε τα εξής:

- Ημερομηνία περιστατικού δεδομένων:
- Όνομα προμηθευτή:
- Αριθμός προμηθευτή:
- Επαφές Microsoft που έχουν ενημερωθεί σχετικά:
- Συσχετισμένη εντολή αγοράς, αν ισχύει/διατίθεται:
- Σύνοψη του Περιστατικού δεδομένων:

Παράρτημα Α:

Απαιτήσεις βάσει εγκρίσεων προφίλ

Αρ.	Προφίλ	Απαιτήσεις διασφάλισης	Επιλογές ανεξάρτητης διασφάλισης
1	**Εμβέλεια**: Προσωπικό, Εμπιστευτικό **Τοποθεσία επεξεργασίας:** Στη Microsoft ή στον Πελάτη **Ρόλος επεξεργασίας:** Εργολάβος επεξεργασίας ή Υπεύθυνος επεξεργασίας **Κατηγορία δεδομένων:** Εμπιστευτικό **ή** Αυστηρά εμπιστευτικό **Κάρτες πληρωμής:** Δεν εφαρμόζεται **SaaS:** Δεν εφαρμόζεται **Χρήση υπεργολάβων:** Δεν εφαρμόζεται **Φιλοξενία ιστότοπων:** Δεν εφαρμόζεται	Αυτοβεβαίωση συμμόρφωσης με το DPR	
2	**Εμβέλεια:** Εμπιστευτικό **Τοποθεσία επεξεργασίας:** Στον Προμηθευτή **Ρόλος επεξεργασίας:** Δεν εφαρμόζεται **Κατηγορία δεδομένων:** Εμπιστευτικό **Κάρτες πληρωμής:** Δεν εφαρμόζεται **SaaS:** Δεν εφαρμόζεται **Χρήση υπεργολάβων:** Δεν εφαρμόζεται **Φιλοξενία ιστότοπων:** Δεν εφαρμόζεται	Αυτοβεβαίωση συμμόρφωσης με το DPR	
3	**Εμβέλεια**: Εμπιστευτικό **Τοποθεσία επεξεργασίας:** Στον Προμηθευτή **Ρόλος επεξεργασίας:** Εργολάβος επεξεργασίας **Κατηγορία δεδομένων:** Αυστηρά εμπιστευτικό **Κάρτες πληρωμής:** Δεν εφαρμόζεται **SaaS:** Δεν εφαρμόζεται **Χρήση υπεργολάβων:** Δεν εφαρμόζεται **Φιλοξενία ιστότοπων:** Δεν εφαρμόζεται	Αυτοβεβαίωση συμμόρφωσης με το DPR **και** Ανεξάρτητη διασφάλιση συμμόρφωσης	Επιλογές ανεξάρτητης διασφάλισης: 1. Ολοκλήρωση μιας Ανεξάρτητης αξιολόγησης έναντι του DPR, **ή** 2. Υποβολή ISO 27001

Αρ.	Προφίλ	Απαιτήσεις διασφάλισης	Επιλογές ανεξάρτητης διασφάλισης
4	**Εμβέλεια:** Προσωπικό, Εμπιστευτικό **Τοποθεσία επεξεργασίας:** Στον Προμηθευτή **Ρόλος επεξεργασίας:** Εργολάβος επεξεργασίας **Κατηγορία δεδομένων:** Αυστηρά εμπιστευτικό **Κάρτες πληρωμής:** Δεν εφαρμόζεται **SaaS:** Δεν εφαρμόζεται **Χρήση υπεργολάβων:** Δεν εφαρμόζεται **Φιλοξενία ιστότοπων:** Δεν εφαρμόζεται	Αυτοβεβαίωση συμμόρφωσης με το DPR **και** Ανεξάρτητη διασφάλιση συμμόρφωσης	Επιλογές ανεξάρτητης διασφάλισης: 1. Ολοκλήρωση μιας Ανεξάρτητης αξιολόγησης έναντι του DPR, 2. Ανεξάρτητη αξιολόγηση σε σχέση με τις ενότητες A-I του DPR και το πρότυπο ISO 27001, **ή** 3. Υποβολή ISO 27701 **και** ISO 27001
5	**Εμβέλεια:** Προσωπικό, Εμπιστευτικό **Τοποθεσία επεξεργασίας:** Στον Προμηθευτή **Ρόλος επεξεργασίας:** Εργολάβος επεξεργασίας **Κατηγορία δεδομένων:** Εμπιστευτικό **Κάρτες πληρωμής:** Δεν εφαρμόζεται **SaaS:** Δεν εφαρμόζεται **Χρήση υπεργολάβων:** Δεν εφαρμόζεται **Φιλοξενία ιστότοπων:** Δεν εφαρμόζεται	Αυτοβεβαίωση συμμόρφωσης με το DPR	
6	**Εμβέλεια:** Προσωπικό, Εμπιστευτικό **Τοποθεσία επεξεργασίας:** Στον Προμηθευτή **Ρόλος επεξεργασίας:** Χειριστήριο **Κατηγορία δεδομένων:** Αυστηρά εμπιστευτικό ή Εμπιστευτικό **Κάρτες πληρωμής:** Δεν εφαρμόζεται **SaaS:** Δεν εφαρμόζεται **Χρήση υπεργολάβων:** Δεν εφαρμόζεται **Φιλοξενία ιστότοπων:** Δεν εφαρμόζεται	Αυτοβεβαίωση συμμόρφωσης με το DPR	

Αρ.	Προφίλ	Απαιτήσεις διασφάλισης	Επιλογές ανεξάρτητης διασφάλισης
7	**Εμβέλεια:** Προσωπικό, Εμπιστευτικό **Τοποθεσία επεξεργασίας:** Οποιαδήποτε **Ρόλος επεξεργασίας:** Υπεργολάβος επεξεργασίας (αυτός ο ρόλος προσδιορίζεται από τη Microsoft – στο προφίλ θα αναγράφεται «Έγκριση υπεργολάβου επεξεργασίας: Ναι») **Κατηγορία δεδομένων:** Αυστηρά εμπιστευτικό ή Εμπιστευτικό **Κάρτες πληρωμής:** Δεν εφαρμόζεται **SaaS:** Δεν εφαρμόζεται **Χρήση υπεργολάβων:** Δεν εφαρμόζεται **Φιλοξενία ιστότοπων:** Δεν εφαρμόζεται	Αυτοβεβαίωση συμμόρφωσης με το DPR **και** Ανεξάρτητη διασφάλιση συμμόρφωσης	Επιλογές ανεξάρτητης διασφάλισης: 1. Ολοκλήρωση μιας Ανεξάρτητης αξιολόγησης έναντι του DPR, 2. Ανεξάρτητη αξιολόγηση σε σχέση με τις ενότητες A-I του DPR και το πρότυπο ISO 27001, **ή** 3. Υποβολή ISO 27701 **και** ISO 27001

Αρ.	Προφίλ	Απαιτήσεις διασφάλισης	Επιλογές ανεξάρτητης διασφάλισης
Αντίκτυπος της προσθήκης SaaS, Υπεργολάβων, Φιλοξενίας ιστότοπων			
8	**Εμβέλεια:** Προσωπικό, Εμπιστευτικό **Τοποθεσία επεξεργασίας:** Στον Προμηθευτή **Ρόλος επεξεργασίας:** Εργολάβος επεξεργασίας **Κατηγορία δεδομένων:** Αυστηρά εμπιστευτικό ή Εμπιστευτικό **Κάρτες πληρωμής:** Δεν εφαρμόζεται **Υπεργολάβοι:** ΝΑΙ ή **SaaS:** ΝΑΙ ή **Φιλοξενία ιστότοπων:** ΝΑΙ	Αυτοβεβαίωση συμμόρφωσης με το DPR **και** Ανεξάρτητη διασφάλιση συμμόρφωσης	Επιλογές ανεξάρτητης διασφάλισης: 1. Ολοκλήρωση μιας Ανεξάρτητης αξιολόγησης έναντι του DPR, 2. Ανεξάρτητη αξιολόγηση σε σχέση με τις ενότητες A-I του DPR και το πρότυπο ISO 27001, **ή** 3. Υποβολή ISO 27701 **και** ISO 27001
9	**Εμβέλεια:** Προσωπικό, Εμπιστευτικό **Τοποθεσία επεξεργασίας:** Στον Προμηθευτή **Ρόλος επεξεργασίας:** Χειριστήριο **Κατηγορία δεδομένων:** Αυστηρά εμπιστευτικό ή Εμπιστευτικό **Κάρτες πληρωμής:** Δεν εφαρμόζεται **Υπεργολάβοι:** ΝΑΙ ή **SaaS:** ΝΑΙ ή **Φιλοξενία ιστότοπων:** ΝΑΙ	Αυτοβεβαίωση συμμόρφωσης με το DPR	

Αρ.	Προφίλ	Απαιτήσεις διασφάλισης	Επιλογές ανεξάρτητης διασφάλισης
Πρόσθετη διασφάλιση για Κάρτες πληρωμής και SaaS			
10	Οποιοδήποτε από τα παραπάνω προφίλ και **Κάρτες πληρωμής**	Παραπάνω ισχύουσες απαιτήσεις **και** διασφάλιση Κλάδου καρτών πληρωμής	Υποβολή πιστοποίησης PCI DSS
11	Οποιαδήποτε από τα παραπάνω προφίλ και **Λογισμικό ως Υπηρεσία (SaaS)**	Παραπάνω ισχύουσες απαιτήσεις **και** πρέπει να υποβάλετε τη συμβατικά απαιτούμενη πιστοποίηση ISO 27001 που καλύπτει τις λειτουργικές υπηρεσίες.	Υποβολή πιστοποίησης ISO 27001 με λειτουργική κάλυψη των παρεχόμενων υπηρεσιών.