ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΝΟΜΙΚΕΣ ΚΑΙ ΟΙΚΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΝΕΦΟΥΣ

Διπλωματική Εργασία

της

Ευθυμίας Α. Μοσχίδου

Θεσσαλονίκη, 1/2022

ΝΟΜΙΚΕΣ ΚΑΙ ΟΙΚΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΗΣ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΝΕΦΟΥΣ

Ευθυμία Α. Μοσχίδου

Πτυχίο Νομικής, Α.Π.Θ. , 2003

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Εμμανουήλ Στειακάκης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 28/02/2022

Εμμανουήλ Στειακάκης Φώτιος Κίτσιος Θεοχάρης Δαλακούρας

Ευθυμία Α. Μοσχίδου

Περίληψη

Στην παρούσα μελέτη, μετά από βιβλιογραφική έρευνα, μελετώνται οι νομικές και οικονομικές επιπτώσεις της υπολογιστικής νέφους. Αρχικά δίνεται ο ορισμός, τα χαρακτηριστικά, οι τεχνικές εκδοχές και τα μοντέλα ανάπτυξης του υπολογιστικού νέφους. Ακολουθεί η διερεύνηση του προσδιορισμού της ιδιότητας των παρόχων υπηρεσιών υπολογιστικού νέφους ως υπεύθυνων επεξεργασίας ή ως εκτελούντων την επεξεργασία προσωπικών δεδομένων και η απόδοση των αντίστοιχων υποχρεώσεων και ευθυνών. Στη συνέχεια αναλύεται το πεδίο εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ) και η βάσει αυτού συγκρότηση του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων (ΕΣΠΔ). Αμέσως μετά ερευνάται και καταγράφεται η εξέλιξη και η ρύθμιση των διασυνοριακών ροών δεδομένων, δεδομένου του «ατοπικού» χαρακτήρα του υπολογιστικού νέφους. Αναλύονται συμφωνίες μεταξύ της ΕΕ και των ΗΠΑ, πως λειτούργησαν και πως τελικά καταργήθηκαν μετά την έκδοση κομβικών δικαστικών αποφάσεων του ΔΕΕ. Το επόμενο μέρος της μελέτης αφορά την παρουσίαση των πιο πρόσφατων και επικαιροποιημένων νομικών μέσων συμμόρφωσης και εφαρμογής του ΓΚΠΔ, όπως ενδεικτικά είναι το νέο τροποποιημένο ISO/IEC 27018:2019, οι νέες τυποποιημένες συμβατικές ρήτρες της ΕΕ, οι δεσμευτικοί εταιρικοί κανόνες και οι κώδικες δεοντολογίας, που εγκρίθηκαν από αρμόδιες εθνικές Εποπτικές Αρχές, αφού έλαβαν θετική γνώμη από το ΕΣΠΔ. Τα νομικά αυτά μέσα έχουν πολλά να εισφέρουν και στο πλαίσιο της κατάρτισης και της λειτουργίας των συμβάσεων υπολογιστικού νέφους που συνάπτονται μεταξύ των εμπλεκομένων-συμβαλλομένων μερών, σε συνδυασμό με τις συμφωνίες επιπέδου υπηρεσιών που συμπεριλαμβάνονται συχνά στις συμβάσεις. Ο νομικός χαρακτηρισμός των συμβάσεων υπολογιστικού νέφους είναι ένα ακόμη σημείο μελέτης της παρούσας διπλωματικής, με τις συνακόλουθες προεκτάσεις του εφαρμοστέου δικαίου και της δικαιοδοσίας. Καταγράφονται επίσης κάποια βασικά χαρακτηριστικά που πρέπει να πληρεί το υπολογιστικό νέφος ως προς το ζήτημα της ασφάλειας. Στο μέρος των οικονομικών επιπτώσεων αποτυπώνεται η διαρκής και ραγδαία ζήτηση υπηρεσιών υπολογιστικού νέφους, η οποία επιφέρει και μεγάλη οικονομική ανάπτυξη στην αγορά παροχής αυτών των υπηρεσιών. Μελετώνται τα πλεονεκτήματα και οι προκλήσεις από τη χρήση υπηρεσιών υπολογιστικού νέφους και προτείνονται κριτήρια αξιολόγησης, λήψης απόφασης και υιοθέτησης εφαρμογών υπολογιστικού νέφους. Τέλος υπάρχει αναφορά στις τρέχουσες κοινωνικές και πολιτικές

εξελίξεις, όπως αυτές εκφράζονται μέσα από τη δραστηριοποίηση, τη λήψη πρωτοβουλιών και τη δημιουργία συμμαχιών από την Ε.Ε. Η παρούσα διπλωματική ολοκληρώνεται με τα συμπεράσματα επί των θεμάτων που μελετήθηκαν.

Λέξεις Κλειδιά: υπολογιστική νέφους, ΓΚΠΔ, πάροχος υπηρεσιών νέφους, διασυνοριακές ροές δεδομένων.

Abstract

In the present study, after bibliographic research, the legal and economic implications of cloud computing are studied. First the definition, the characteristics, the technical versions and the development models of the cloud computing are given. The following is the investigation of the definition of the status of cloud computing service providers as controller or processor in the processing of personal data and the performance of the respective obligations and responsibilities. Then the field of application of the General Data Protection Regulation (GDPR) and the establishment of the European Data Protection Council (EDPB) are analyzed. Right after, the evolution and regulation of cross-border data flows are investigated and recorded, given the atopic nature of the cloud computing. Agreements between the EU and the US are analyzed, how they worked and how they were finally abolished after the issue of key court decisions of the CJEU. The next part of the study concerns the presentation of the most recent and up-to-date legal instruments for compliance and implementation with the GDPR, such as the newly amended ISO / IEC 27018: 2019, the new standard contractual clauses of EU, the binding corporate rules and codes of conduct, approved by competent national Supervisory Authorities, after receiving a positive opinion from the EDPB. These legal instruments also have much to contribute to the drawing up and the operation of cloud computing contracts concluded between the parties involved, in conjunction with the service level agreements that often included in the contracts. The legal characterization of cloud computing contracts is another point of study hereof, with the consequent extensions of applicable law and jurisdiction. It also lists some key features that the cloud computing must meet in terms of security. The part of the financial implications reflects the continuous and rapid demand for cloud computing services, which also leads to great economic growth in the market for the provision of these services. The advantages and challenges of using cloud computing services are studied and criteria for evaluating, deciding and adopting cloud computing applications are proposed. Finally, there is a reference to current social and political developments, as expressed through activation, taking initiatives and the creation of alliances by the EU. The present thesis concludes with the conclusions on the subjects that were studied.

Keywords: cloud computing, GDPR, cloud service provider, cross-border data flows.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κ. Εμμανουήλ Στειακάκη, Καθηγητή του Τμήματος Εφαρμοσμένης Πληροφορικής του Πανεπιστημίου Μακεδονίας, για τη συνεργασία και την επικοινωνία, καθώς και για τις χρήσιμες παρατηρήσεις και συμβουλές που μου έδωσε κατά την συγγραφή της παρούσας διπλωματικής εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τον σύζυγο, τα παιδιά και τους γονείς μου για την πολύτιμη βοήθεια, στήριξη και κατανόηση που έδειξαν όλο αυτό το χρονικό διάστημα έρευνας και συγγραφής της παρούσας διπλωματικής εργασίας μου.

Πίνακας Περιεχομένων

Κατάλογος Πινάκων

Κατάλογος γραφημάτων

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

Βλ.: Βλέπε

παρ. : παράγραφος

ΓΚΠΔ: Γενικός Κανονισμός Προστασίας Δεδομένων

Εισ. Σκ. : Εισαγωγική Σκέψη

Ε.Ε.: Ευρωπαϊκή Ένωση

Δ.Ε.Ε.: Δικαστήριο Ευρωπαϊκής Ένωσης

Ε..Ο.Χ.: Ευρωπαϊκός Οικονομικός Χώρος

ΑΠΔΠΧ: Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΤΠΕ: Τεχνολογίες της Πληροφορικής και των Επικοινωνιών

ΕΣΠΔ: Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

ΜΜΕ: Μικρο-Μεσαίες Επιχειρήσεις

IT : Information Technology

SaaS: Software as a Service

PaaS: Platform as a service

IaaS: Infrastructure as a service

SLA: Service Level Agreement

CSP: Cloud Service Provider (Πάροχος Υπηρεσιών Νέφους)

CSC: Cloud Service Consumer (Πελάτης Υπηρεσιών Νέφους)

SCC: Standard Contractual Clauses (Τυπικές Συμβατικές Ρήτρες)

BCR: Binding Corporate Rules (Δεσμευτικοί Εταιρικοί Κανόνες)

CoC: Code of Conduct (Κώδικας Δεοντολογίας)

ENISA: European Union Agency for Cybersecurity (Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια)

CISPE: Cloud Infrastructure Service Providers Europe (Πάροχοι Υπηρεσιών Υποδομής Νέφους Ευρώπης)

FR SA: French Supervising Authority

CNIL: Εθνική Επιτροπή Υπολογιστών και Ελευθεριών της Γαλλίας

PII : Personally Identifiable Information (Προσωπικές Αναγνωριστικές Πληροφορίες)

ISO: International Organization for Standardization

CIA: Confidentiality – Integrity - Availability (Εμπιστευτικότητα - Ακεραιότητα - Διαθεσιμότητα)

1 Εισαγωγή

Σήμερα, περισσότερο από ποτέ, καθώς μαίνεται ακόμη η πανδημία λόγω covid-19 και έχει επιφέρει μια σειρά ραγδαίων κοινωνικών, νομικών και οικονομικών εξελίξεων, ο τομέας των Τεχνολογιών της Πληροφορικής και των Επικοινωνιών (ΤΠΕ) καταλαμβάνει κυρίαρχο ρόλο σε όλες τις πτυχές της καθημερινότητας του σύγχρονου ανθρώπου. Από αυτές τις τεχνολογίες ξεχωρίζει και είναι ιδιαίτερα σημαντικό το υπολογιστικό νέφος (cloud computing), το οποίο με τη σειρά του καταλαμβάνει ένα μεγάλο μέρος της λειτουργίας του διαδικτύου.

Το υπολογιστικό νέφος αλλάζει τα δεδομένα στη διακίνηση, στη διαχείριση, στην αποθήκευση των πληροφοριακών δεδομένων, αλλά και γενικά στη λειτουργία της σύγχρονης πληροφορικής τεχνολογίας(Information Technology, IT). Στις 19 Ιουλίου 2021 εγκαινιάστηκε από την Ευρωπαϊκή Επιτροπή η ευρωπαϊκή συμμαχία για τα βιομηχανικά δεδομένα, τις παρυφές και το υπολογιστικό νέφος, που αναμένεται «να προωθήσει την εμφάνιση ανατρεπτικών τεχνολογιών στον εν λόγω κλάδο, που θα είναι υψηλής ασφάλειας, αποδοτικές ως προς την ενέργεια και τη χρήση των πόρων και πλήρως διαλειτουργικές, ενώ θα ενισχύσει την εμπιστοσύνη των χρηστών του υπολογιστικού νέφους σε όλους τους τομείς». Η Ευρώπη επιθυμεί και επιδιώκει να επιτελέσει σημαντικό ρόλο στη σύγχρονη ψηφιακή αγορά και μέσω της τεχνολογίας του υπολογιστικού νέφους.

Χάρη στα πολλά πλεονεκτήματα που παρουσιάζει το υπολογιστικό νέφος, όπως ευελιξία, γεωγραφική ανεξαρτησία, αμεσότητα, ταχύτητα και προσαρμοστικότητα, υιοθετείται ολοένα και περισσότερο από απλούς χρήστες-καταναλωτές, επιχειρήσεις, οργανισμούς, κυβερνήσεις και κράτη. Αυτό βέβαια δεν σημαίνει πως δεν παρουσιάζει και μειονεκτήματα-προκλήσεις, η διαχείριση των οποίων αποτελεί αντικείμενο επιστημονικής μελέτης. Από την εφαρμογή του τίθενται σοβαρά νομικά ζητήματα προς αντιμετώπιση, ρύθμιση και επίλυση. Στην παρούσα διπλωματική στόχος είναι να γίνει μια καταγραφή και ανάλυση των διαθέσιμων και επικαιροποιημένων μέσων συμμόρφωσης και εφαρμογής του ΓΚΠΔ για την προστασία των προσωπικών δεδομένων των υποκειμένων που καταχωρούνται, επεξεργάζονται, μεταφέρονται και αποθηκεύονται στο υπολογιστικό νέφος κι επομένως μέσω αυτού οπουδήποτε στον κόσμο. Μεταξύ των επικαιροποιημένων μέσων ξεχωρίζουν οι νέες τυποποιημένες

συμβατικές ρήτρες της Ε.Ε. , νέοι Ευρωπαϊκοί κώδικες δεοντολογίας, αναθεωρημένα πρότυπα πιστοποίησης, αλλά και κομβικές δικαστικές αποφάσεις του ΔΕΕ. Στόχος είναι η αξιοποίηση και εφαρμογή αυτών για να διαμορφωθούν κατάλληλες και επικαιροποιημένες συμβάσεις υπολογιστικού νέφους, ώστε η κατάρτιση και η τήρησή τους να καλλιεργήσει ένα κλίμα εμπιστοσύνης και αξιοπιστίας στους χρήστες-πελάτες υπέρ των παρόχων υπηρεσιών υπολογιστικού νέφους και εν γένει της τεχνολογίας υπολογιστικού νέφους, προσφέροντας περισσότερες εγγυήσεις ασφάλειας και εμπιστευτικότητας. Με βάση το νομικό χαρακτηρισμό των συμβάσεων υπολογιστικού νέφους και την υπαγωγή τους στους αντίστοιχους κανόνες δικαίου, κρίνεται και ερευνάται το ζήτημα της διεθνούς δικαιοδοσίας.

Η υιοθέτηση και χρήση των υπηρεσιών υπολογιστικού νέφους από απλούς χρήστες έως μεγάλους ομίλους επιχειρήσεων αλλά και από τα ίδια τα κράτη έχει και οικονομικές διαστάσεις. Καταγράφεται σταθερά αυξητική τάση τα τελευταία χρόνια. Παρουσιάζεται μεγάλο οικονομικό ενδιαφέρον γύρω από τον επιχειρηματικό κλάδο της τεχνολογίας υπολογιστικού νέφους και της παροχής υπηρεσιών νέφους. Οι πελάτες των υπηρεσιών αυτών πρέπει να χρησιμοποιούν κριτήρια στην επιλογή των κατάλληλων για αυτούς και τις ανάγκες τους υπηρεσιών νέφους. Δεν πρέπει να παραλείπουν να προσμετρούν πέρα από τα πλεονεκτήματα και τις προκλήσεις που έχει η αξιοποίηση της τεχνολογίας του υπολογιστικού νέφους.

2 Υπηρεσίες Cloud Computing

2.1 Η έννοια του υπολογιστικού νέφους

Καθώς συγκεντρώνει τόσο μεγάλο ενδιαφέρον ως τεχνολογία αιχμής το υπολογιστικό νέφος, είναι πολλοί και οι επιχειρούμενοι ορισμοί του. Μεταξύ αυτών έχει ξεχωρίσει ως πληρέστερος αυτός που διατύπωσε το Εθνικό Ίδρυμα Προτύπων και Τεχνολογίας των ΗΠΑ (U.S. National Institute of Standards and Technology, NIST): το υπολογιστικό νέφος είναι ένα μοντέλο, το οποίο παρέχει τη δυνατότητα ευχερούς, βασισμένης στη ζήτηση διαδικτυακής πρόσβασης σε ένα διαμοιραζόμενο χώρο (π.χ. δίκτυα, εξυπηρετητές, αποθήκευση, εφαρμογές και υπηρεσίες) και το οποίο μπορεί να παρασχεθεί και να αποδεσμευτεί ταχέως με ελάχιστη διαχειριστική προσπάθεια ή αλληλεπίδραση με τον πάροχο της υπηρεσίας[1].

Από την άλλη, η Ευρωπαϊκή Επιτροπή στην ανακοίνωσή της στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών για την «Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους στην Ευρώπη» αναφέρει ότι «το "υπολογιστικό νέφος" μπορεί να γίνει κατανοητό με απλό τρόπο ως αποθήκευση, επεξεργασία και χρήση δεδομένων σε απομακρυσμένους υπολογιστές που είναι προσβάσιμοι μέσω του διαδικτύου. Αυτό σημαίνει ότι οι χρήστες έχουν στη διάθεσή τους σχεδόν απεριόριστη υπολογιστική ισχύ σε πρώτη ζήτηση, ότι δεν υποχρεώνονται σε μεγάλες επενδύσεις κεφαλαίων ώστε να καλύψουν τις ανάγκες τους και ότι μπορούν να αντλήσουν τα δεδομένα τους από οπουδήποτε μέσω διαδικτυακής σύνδεσης. Το υπολογιστικό νέφος έχει τη δυνατότητα να μειώσει δραστικά τις δαπάνες τεχνολογίας πληροφοριών (ΤΠ) των χρηστών και να καταστήσει δυνατή την ανάπτυξη πολλών νέων υπηρεσιών. Χρησιμοποιώντας το υπολογιστικό νέφος, ακόμη και οι μικρότερες εταιρίες μπορούν να εισέλθουν σε συνεχώς μεγαλύτερες αγορές, ενώ οι κυβερνήσεις μπορούν να κάνουν τις υπηρεσίες τους πιο ελκυστικές και αποτελεσματικές, με παράλληλη τιθάσευση των δαπανών»[2,3].

[1] Peter Mell (NIST), Tim Grance (NIST), Ορισμός του NIST National Institute of Standards and Technology (Σεπτέμβριος 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final

[2] S. Ahmed, Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 6/2014, Ιούνιος 2014.

[3] Ανακοίνωση της Ευρωπαϊκής Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών για την «Αξιοποίηση των

2.2 Χαρακτηριστικά του υπολογιστικού νέφους

Το υπολογιστικό νέφος χαρακτηρίζεται από[4]:

«1. Αυτο-εξυπηρέτηση κατά απαίτηση (on-demand self-service): Ένας καταναλωτής μπορεί μονομερώς να έχει παροχή υπολογιστικών δυνατοτήτων, όπως π.χ. είναι ο χρόνος διακομιστή και η αποθήκευση δικτύου, όπως απαιτείται αυτόματα, χωρίς να απαιτείται ανθρώπινη αλληλεπίδραση με κάθε πάροχο υπηρεσιών.

2. Ευρεία πρόσβαση στο δίκτυο (Broad network access): Οι δυνατότητες είναι διαθέσιμες μέσω του δικτύου και προσβάσιμες μέσω τυποποιημένων μηχανισμών που προωθούν τη χρήση με ετερογενείς λεπτές ή παχιές πλατφόρμες πελατών (π.χ. κινητά τηλέφωνα, tablet, φορητούς υπολογιστές και σταθμούς εργασίας).

3. Διάθεση πόρων (resource pooling): Οι υπολογιστικοί πόροι του παρόχου συγκεντρώνονται για να εξυπηρετούν πολλαπλούς χρήστες ταυτόχρονα, χρησιμοποιώντας ένα μοντέλο πολλαπλών μισθωτών, εκχωρούνται δυναμικά με διαφορετικούς φυσικούς και εικονικούς πόρους και ανάλογα με την καταναλωτική ζήτηση. Υπάρχει μια αίσθηση τοποθεσίας ανεξάρτητα από το ότι ο πελάτης γενικά δεν έχει κανέναν έλεγχο ή γνώση σχετικά με την ακριβή τοποθεσία των παρεχόμενων πόρων, αλλά μπορεί να είναι σε θέση να καθορίσει την τοποθεσία σε ένα υψηλότερο επίπεδο αφαίρεσης (π.χ. χώρα, πολιτεία ή κέντρο δεδομένων). Παραδείγματα πόρων περιλαμβάνουν την αποθήκευση, επεξεργασία, μνήμη και εύρος ζώνης δικτύου.

4. Ταχεία ελαστικότητα/ επεκτασιμότητα υπηρεσίας μέσω ανακατανομής πόρων (rapid elasticity): Οι δυνατότητες μπορούν να παρέχονται και να απελευθερώνονται ελαστικά, σε ορισμένες περιπτώσεις αυτόματα, να κλιμακώνεται γρήγορα προς τα έξω και προς τα μέσα ανάλογα με τη ζήτηση. Στον καταναλωτή, οι δυνατότητες που είναι διαθέσιμες

δυνατοτήτων του υπολογιστικού νέφους», COM(2012)529nal, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EL:PDF

[4] Peter Mell (NIST), Tim Grance (NIST), Ορισμός του NIST National Institute of Standards and Technology (Σεπτέμβριος 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final

για παροχή, συχνά φαίνονται απεριόριστες και μπορούν να διατίθενται σε οποιαδήποτε ποσότητα ανά πάσα στιγμή.

5. Μετρούμενη υπηρεσία (measured service): Τα συστήματα Cloud ελέγχουν και βελτιστοποιούν αυτόματα τη διάθεση των πόρων παρέχοντας τη δυνατότητα μέτρησης των χρησιμοποιούμενων υπηρεσιών ανάλογα με το είδος (π.χ. λογαριασμοί αποθήκευσης, επεξεργασίας, εύρους σύνδεσης ή διαθέσιμων λογαριασμών χρηστών). Η χρήση πόρων μπορεί να παρακολουθείται, να ελέγχεται και να αναφέρεται, παρέχοντας διαφάνεια τόσο για τον πάροχο όσο και για τον καταναλωτή της χρησιμοποιούμενης υπηρεσίας».

Τα χαρακτηριστικά αυτά συμπληρώνονται και από τις εξής ιδιότητες που εμφανίζει η λειτουργία του:
-Συγκέντρωση και διαθεσιμότητα υπολογιστικών πόρων κάθε επιπέδου ανεξάρτητα από εντοπιότητα χρήστη (location independence).
- Χρήση υπολογιστικών πόρων ανεξάρτητα από εντοπιότητα αυτών.
- Δυνατότητα κλωνοποίησης: σε περιπτώσεις που απαιτείται μεγαλύτερη ταχύτητα πρόσβασης (live streaming, streamed video gaming κλπ) υπάρχει δυνατότητα οι υπολογιστικοί πόροι να κλωνοποιούνται σε περιοχές κοντά στον τελικό χρήστη.

2.3 Τεχνικές εκδοχές υπολογιστικού νέφους βάσει των παρεχόμενων υπηρεσιών

Το υπολογιστικό νέφος διακρίνεται βάσει των παρεχόμενων μέσω αυτού υπηρεσιών σε τρεις τεχνικές εκδοχές που οδηγούν στην ανάπτυξη τριών αντίστοιχων επιχειρηματικών μοντέλων[5]:

Α). Το Λογισμικό-ως-Υπηρεσία (Software-as-a-Service – SaaS).
Στο SaaS ο πάροχος εκμισθώνει στον πελάτη του λογισμικό. Δηλαδή, ο χρήστης του λογισμικού, αντί να το αγοράζει και να το εγκαθιστά στο πληροφορικό του σύστημα,

[5] Dr. Konstantinos E. Psannis, University of Macedonia, Greece, Lecture Cloud Computing http://compus.uom.gr/MLI4/document/Dialeksh_02/Lect-Cloud-2017.pdf (σελ. 27-34)

το μισθώνει ως υπηρεσία από τον πάροχο του λογισμικού μέσω του συστήματος της υπολογιστικής νέφους. Αποτελεί μοντέλο παροχής λογισμικού με λειτουργικότητα παρόμοια με εκείνη της εφαρμογής τελικού χρήστη [όπως τα Microsoft Office 365, Microsoft Dynamics CRM, Google Docs]. Οι πάροχοι προσφέρουν διάφορες υπηρεσίες εφαρμογών, στις οποίες οι τελικοί χρήστες έχουν πρόσβαση μέσω φυλλομετρητή (browser) στο Διαδίκτυο και μπορούν να αντικαταστήσουν συμβατικές εφαρμογές εγκατεστημένες σε τοπικά συστήματα.

Παραδείγματα υπηρεσίας υπολογιστικού νέφους που προσφέρεται ως λογισμικό αποτελεί το ηλεκτρονικό ταχυδρομείο, οι εφαρμογές κινητής τηλεφωνίας, το Dropbox, google docs.

Β). Η Πλατφόρμα-ως-Υπηρεσία (Platform-as-a-Service – PaaS).

Στην PaaS ο πάροχος εκμισθώνει στον πελάτη του μια πλατφόρμα υπολογιστικών εφαρμογών -του παρέχει δηλαδή τα εργαλεία- για την κατασκευή, την αποθήκευση και τη χρήση στο υπολογιστικό νέφος συγκεκριμένων διαδικτυακών εφαρμογών που δημιουργεί ο πελάτης. Έτσι, ο πελάτης είναι υπεύθυνος αποκλειστικά για το λογισμικό, ενώ ο πάροχος φροντίζει για την 24ωρη διαθεσιμότητα του υλικού, τη σωστή του λειτουργία, καθώς και τη συντήρηση της πλατφόρμας πάνω στην οποία εκτελείται το λογισμικό. Απευθύνεται κυρίως σε προγραμματιστές για την ανάπτυξη εφαρμογών, καλύπτοντας τις τεχνικής φύσεως ανάγκες που υπάρχουν. Οι προγραμματιστές χρησιμοποιώντας την πλατφόρμα, η οποία μπορεί να παραμετροποιηθεί ή να προσαρμοστεί ανάλογα με τις ανάγκες τους, προχωρούν στη συγγραφή του κώδικα. Παραδείγματα είναι το Mozilla, το Google App Engine, το Microsoft Windows Azure, Youtube και το Bespin[6].

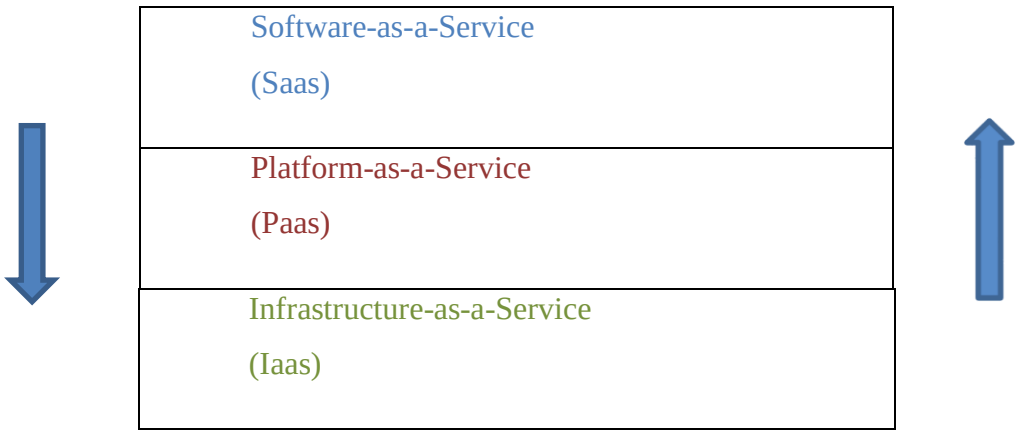
Γ). Η Υποδομή-ως-Υπηρεσία (Infrastructure-as-a-Service – IaaS).

Στην IaaS ο πάροχος εκμισθώνει στον πελάτη του μία υπολογιστική υποδομή εικονικών εξυπηρετητών που μπορεί να περιλαμβάνει υπολογιστική ισχύ, υπολογιστική αποθήκευση (hosting), χρήση εξυπηρετητή (server), χρήση κέντρου δεδομένων (data center), υπολογιστικό δίκτυο (network) κ.λπ. που απλοποιούν,

[6] Dr. Konstantinos E. Psannis, University of Macedonia, Greece, Lecture Cloud Computing http://compus.uom.gr/MLI4/document/Dialeksh_02/Lect-Cloud-2017.pdf (σελ.32)

καθιστούν αποτελεσματική και ευνοούν την υποκατάσταση των εταιρικών συστημάτων τεχνολογιών της πληροφορίας στις εγκαταστάσεις της επιχείρησης του πελάτη ή/και τη χρήση της μισθωμένης υποδομής παράλληλα με τα εταιρικά του συστήματα. Σε αυτήν την εκδοχή, ο παρέχων την υπηρεσία εγγυάται συνήθως τη συνεχή λειτουργία των συστημάτων, άλλες λειτουργίες όμως, όπως για παράδειγμα, η εγκατάσταση και ρύθμιση του λογισμικού, η συντήρηση και παρακολούθησή του και η δημιουργία αντιγράφων ασφαλείας, είναι καθαρά ευθύνη του πελάτη. Η εν λόγω υπηρεσία απευθύνεται κυρίως σε τελικούς χρήστες, καταναλωτές. Παράδειγμα αποτελούν οι διαδικτυακές υπηρεσίες της Amazon.

SPI Model (αρχικά των λέξεων software, platform, infrastructure)

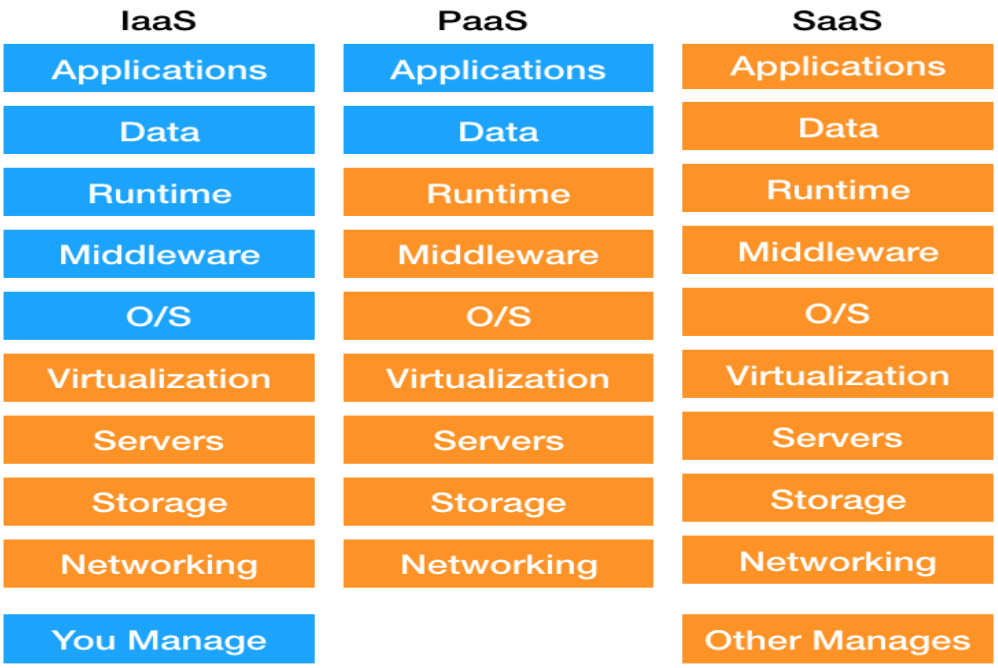


Πίνακας 1 : SPI Model

Το αριστερό βελάκι δείχνει την ευελιξία του καταναλωτή, η οποία αυξάνεται από πάνω προς τα κάτω, ενώ το δεξί βελάκι καταδεικνύει την μείωση ελέγχου από τον καταναλωτή με πορεία από κάτω προς τα πάνω.

Πηγή: http://compus.uom.gr/MLI4/document/Dialeksh_02/Lect-Cloud-2017.pdf (σελ.28)[7]

[7]Dr. Konstantinos E. Psannis, University of Macedonia, Greece, Lecture Cloud Computing http://compus.uom.gr/MLI4/document/Dialeksh_02/Lect-Cloud-2017.pdf (σελ.28).



Πίνακας 2: Παρουσίαση τεχνικών εκδοχών υπηρεσιών cloud με την ανάληψη επιμέρους λειτουργιών από παρόχους (CSP) και πελάτες(CSC).
(Εμφανίζεται με γαλάζιο χρώμα κάθε λειτουργία που ανήκει στον πελάτη- CSC (you manage) και με πορτοκαλί χρώμα κάθε λειτουργία που ανήκει στον πάροχο- CSP(other manages))
Πηγή: Από ιστοσελίδα https://reasonstreet.co/infrastructure-as-a-service/

Στην IaaS, ο CSP παρέχει μόνο την υποδομή όπως δίκτυα, αποθήκευση, διακομιστή και εικονικοποίηση. Ο CSC είναι υπεύθυνος για εφαρμογές, δεδομένα, χρόνο εκτέλεσης, ενδιάμεσο λογισμικό και λειτουργικά συστήματα.
Στην PaaS, μόνο οι εφαρμογές και τα δεδομένα είναι ευθύνη του CSC, ενώ οι υπόλοιπες υπηρεσίες παρέχονται από τον CSP.
Στο SaaS, και οι εννέα υπηρεσίες/ λειτουργίες παρέχονται από τον CSP.

Επιπλέον συναντώνται στη βιβλιογραφία και δύο ακόμη μοντέλα παροχής υπηρεσιών υπολογιστικού νέφους: το Hardware as a service (HaaS) και το Database as a service (DaaS)[8].
Στο HaaS ο πάροχος επιτρέπει στους πελάτες να νοικιάζουν hardware, πρόκειται δηλαδή για την ενοικίαση υλικού, που επιτρέπει στους χρήστες τη δημιουργία data centers χωρίς να πρέπει να αγοράσουν το υλικό που απαιτείται. Μπορεί να

[8]Dr. Konstantinos E. Psannis, University of Macedonia, Greece, Lecture Cloud Computing, http://compus.uom.gr/MLI4/document/Dialeksh_02/Lect-Cloud-2017.pdf (σελ.40-43)

χρησιμοποιείται ο εξοπλισμός από πολλαπλούς χρήστες και οι πόροι χρεώνονται ανάλογα με τη χρήση τους.

Στο DaaS επιδίωξη είναι να αποφευχθεί το μεγάλο κόστος για τη λειτουργία μιας ιδιωτικής βάσης δεδομένων, η οποία θα απαιτούσε κάποιο πλεονασματικό σύστημα για να αποθηκευτεί η βάση δεδομένων και να απαιτείται συντήρηση. Ακόμη δεν χρειάζεται να αγοραστεί το σχετικό υλικό, το λογισμικό και να υπάρξει κόστος συντήρησης του υλικού για τη βάση δεδομένων. Στο DaaS δεν υπάρχει τοπικά η βάση δεδομένων, παρολ' αυτά διατηρεί τη λειτουργικότητα και την αποτελεσματικότητά της.

2.4 Μοντέλα ανάπτυξης υπολογιστικού νέφους

Ανάλογα με την εμβέλειά του το υπολογιστικό νέφος μπορεί να είναι:

2.4.1 Ιδιωτικό νέφος (Private Cloud):

Αυτό χρησιμοποιείται αποκλειστικά από συγκεκριμένο οργανισμό (εταιρία, μη κερδοσκοπικό φορέα, νομικό πρόσωπο ιδιωτικού ή δημοσίου δικαίου κ.λπ.). Μπορεί να είναι ιδιόκτητο υπολογιστικό νέφος ή να ανήκει σε τρίτον. Μπορεί να χρησιμοποιεί υπολογιστικούς πόρους εντός ή εκτός του οργανισμού που το χρησιμοποιεί.

2.4.2 Κοινοτικό Νέφος (Community Cloud):

Αυτό χρησιμοποιείται αποκλειστικά από χρήστες που έχουν κοινά συμφέροντα ή ενδιαφέροντα σε επίπεδο οργανισμού (όμιλος εταιριών, κοινότητα χρηστών, περισσότερα νομικά πρόσωπα δημοσίου ή ιδιωτικού δικαίου κ.λπ.). Μπορεί να είναι ιδιόκτητο υπολογιστικό νέφος ενός ή περισσότερων αυτόνομων μονάδων που ανήκουν στον ίδιο οργανισμό ή να ανήκει σε τρίτον. Μπορεί να χρησιμοποιεί υπολογιστικούς πόρους εντός ή εκτός των αυτόνομων μονάδων του οργανισμού που το χρησιμοποιεί.

2.4.3 Δημόσιο Νέφος (Public Cloud):

Αυτό χρησιμοποιείται από οποιονδήποτε σε δημόσιο ή ιδιωτικό χώρο. Μπορεί να ανήκει σε φορέα της ακαδημαϊκής κοινότητας, σε οργανισμό τοπικής αυτοδιοίκησης,

σε νομικό πρόσωπο δημοσίου ή ιδιωτικού δικαίου. Χρησιμοποιεί υπολογιστικούς πόρους που υπάρχουν στον τόπο εγκατάστασης του παρόχου.

2.4.4 Υβριδικό Νέφος (Hybrid Cloud):

Είναι σύνθεση δύο ή περισσότερων διαφορετικών υπολογιστικών νεφών, δηλαδή ιδιωτικού, δημόσιου ή κοινοτικού, που, παρόλο ότι δεν αλλοιώνουν τα χαρακτηριστικά τους ως τέτοια, εντούτοις συνλειτουργούν συνδεόμενα μεταξύ τους επιτρέποντας τη μεταφορά δεδομένων και εφαρμογών από το ένα νέφος στο άλλο.

2.5 Προσδιορισμός ιδιότητας παρόχων υπηρεσιών cloud: υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία

Ιδιαίτερα κρίσιμος είναι ο προσδιορισμός της ιδιότητας των παρόχων υπηρεσιών cloud ως προς την επεξεργασία των προσωπικών δεδομένων προκειμένου να καθοριστούν οι υποχρεώσεις και τα δικαιώματά τους έναντι των πελατών –χρηστών τους. Η απόδοση της έννοιας του υπευθύνου ή του εκτελούντα την επεξεργασία έχει βαρύνουσα σημασία «για τη συμμόρφωση προς τους κανόνες προστασίας των δεδομένων, με ποιον τρόπο τα πρόσωπα στα οποία αναφέρονται τα δεδομένα μπορούν να ασκήσουν τα δικαιώματά τους, ποιο είναι το εφαρμοστέο εθνικό δίκαιο και πώς μπορούν να λειτουργήσουν αποτελεσματικά οι αρχές προστασίας δεδομένων»[9].

Σύμφωνα με το άρθρο 4 παρ. 7 του ΓΚΠΔ ««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».

[9] Ομάδα Άρθρου 29, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου επεξεργασίας» και του «εκτελούντος την επεξεργασία» , WP 169, σελ. 3.

Υπεύθυνος επεξεργασίας είναι οποιοσδήποτε καθορίζει, μόνος του ή από κοινού με άλλους, τον σκοπό και τον τρόπο επεξεργασίας των προσωπικών δεδομένων, και συνακόλουθα φέρει και την ευθύνη για την πραγματοποιούμενη επεξεργασία[10]. Ο υπεύθυνος επεξεργασίας οφείλει να τηρεί κάποιες νόμιμες υποχρεώσεις, βάσει των αρχών νόμιμης επεξεργασίας που θέτει το άρθρο 5 ΓΚΠΔ. Ενδεικτικά οφείλει να τηρεί τις αρχές νόμιμης επεξεργασίας, να λαμβάνει την συγκατάθεση του υποκειμένου των δεδομένων, πλην εξαιρέσεων, να ειδοποιεί την Αρχή για το ότι επεξεργάζεται απλά δεδομένα ή να λαμβάνει άδεια της Αρχής για την επεξεργασία ευαίσθητων δεδομένων, πλην εξαιρέσεων, να ενημερώνει το υποκείμενο των προσωπικών δεδομένων για την επεξεργασία δεδομένων που το αφορούν, να ανταποκρίνεται στην άσκηση των δικαιωμάτων του υποκειμένου όπως πρόσβασης, αντίρρησης, διαγραφής. Ακόμη στα πλαίσια της ευθύνης του πρέπει σύμφωνα με το άρθρο 24 παρ. 1 του ΓΚΠΔ να «εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον παρόντα κανονισμό. Τα εν λόγω μέτρα επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο».

Για την απόδοση του ρόλου του υπευθύνου επεξεργασίας αξιολογείται ο βαθμός λεπτομέρειας καθορισμού των σκοπών και του τρόπου επεξεργασίας. Ο καθορισμός των σκοπών της επεξεργασίας και αποφάσεις όπως ποια δεδομένα θα υποβληθούν σε επεξεργασία, ποιοι μπορούν να έχουν πρόσβαση σε αυτά, πότε θα διαγραφούν τα δεδομένα κ.λπ. λαμβάνονται από τον υπεύθυνο επεξεργασίας.

Σύμφωνα με το άρθρο 4 παρ. 8 του ΓΚΠΔ «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». « Η επεξεργασία από τον εκτελούντα την επεξεργασία διέπεται από σύμβαση ή άλλη νομική πράξη υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους, που δεσμεύει τον εκτελούντα την επεξεργασία σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της επεξεργασίας, το είδος των δεδομένων προσωπικού χαρακτήρα και τις κατηγορίες

[10] Ευγενία Αλεξανδροπούλου – Αιγυπτιάδου, Προσωπικά Δεδομένα, 2016, εκδόσεις Νομική Βιβλιοθήκη, σελ. 61.

των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του υπευθύνου επεξεργασίας…» σύμφωνα με το άρθρο 28 παρ.3 του ΓΚΠΔ. Ο εκτελών την επεξεργασία αναλαμβάνει κατόπιν ανάθεσης του υπευθύνου (μέσω σύναψης σχετικής σύμβασης) την εκτέλεση της επεξεργασίας αναφορικά με τεχνικά και οργανωτικά ζητήματα και σύμφωνα με τις αποφάσεις και εντολές του υπευθύνου, αναλαμβάνει δηλαδή εργασίες όπως συντήρηση λογισμικού ή πλατφόρμας, λήψη αντιγράφων ασφαλείας, κατανομή υπολογιστικών πόρων ανάλογα με τις ανάγκες του πελάτη (On-demand) κ.λπ. Μεταξύ άλλων ο εκτελών την επεξεργασία οφείλει να λαμβάνει όλα τα απαιτούμενα μέτρα ασφαλείας (άρθρο 32 ΓΚΠΔ), να ενημερώνει αμελλητί τον υπεύθυνο επεξεργασίας σε σχέση με την παραβίαση δεδομένων (άρθρο 33 παρ. 2 ΓΚΠΔ), αλλά και να παρέχει τη συνδρομή του σε αυτόν για τη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που αφορούν την κοινοποίηση παραβίασης προσωπικών δεδομένων.

Ο ΓΚΠΔ μάλιστα σε μια προσπάθεια να λύσει το θέμα της διαφάνειας ως προς το πρόσωπο και τις ευθύνες του εκτελούντος την επεξεργασία, ορίζει ότι ο υπεύθυνος επεξεργασίας πρέπει να «χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν αρκετές διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων, κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του παρόντος κανονισμού και να διασφαλίζεται η προστασία των δικαιωμάτων του υποκειμένου των δεδομένων» (άρθρο 28 παρ. 1 ΓΚΠΔ). Από την άλλη μεριά ο ΓΚΠΔ οριοθετεί με πολύ αναλυτικό τρόπο το περιεχόμενο της σύμβασης ή της «άλλης νομικής πράξης» που καθορίζει τις σχέσεις του υπευθύνου την επεξεργασία με τον εκτελούντα αυτή (άρθρο 28 παρ.3).

Είναι πιθανό οι πάροχοι υπηρεσιών cloud να μη γνωρίζουν καθόλου τη λειτουργία των προγραμμάτων που διαχειρίζονται ή το περιεχόμενο των δεδομένων που επεξεργάζονται οι πελάτες τους. Σ’ αυτή την περίπτωση υπεύθυνος επεξεργασίας είναι ο πελάτης των υπηρεσιών cloud και είναι αναμενόμενος ο χαρακτηρισμός του εκτελούντος την επεξεργασία στον πάροχο των υπηρεσιών cloud (υλικού, πλατφόρμας ή λογισμικού), γιατί ακόμη και στην περίπτωση της παροχής υποδομής (IaaS) και μόνον, ο παρέχων την υποδομή έχει τη δυνατότητα να διατηρήσει ή να αποκτήσει πρόσβαση σε αυτήν σε συνδυασμό με το γεγονός ότι ο χρήστης δεν έχει την φυσική εξουσίαση στην υπολογιστική υποδομή των προσωπικών του δεδομένων.

Ακόμη, μπορεί οι πάροχοι υπηρεσιών Cloud να καθορίζουν τον τρόπο της επεξεργασίας υπό μία έννοια π.χ το υλικό (hardware) και να μην θεωρούνται υπεύθυνοι επεξεργασίας αλλά μόνον εκτελούντες την επεξεργασία[11].

Γενικά, η θεωρία και τα θεσμικά όργανα, όπως το Ευρωπαϊκό Κοινοβούλιο ή η Ομάδα του Άρθρου 29[12], τείνουν να αντιλαμβάνονται τους παρόχους υπηρεσιών cloud ως εκτελούντες την επεξεργασία. Πολλοί βέβαια είναι αυτοί που υπογραμμίζουν την ανισότητα διαπραγματευτικής ισχύος των πελατών τέτοιων υπηρεσιών, δεδομένου ότι ο πελάτης είναι σχεδόν υποχρεωμένος να προσχωρεί και να αποδέχεται τους όρους τυποποιημένων συμβάσεων που προτείνουν οι πάροχοι υπηρεσιών cloud. Παρόλ' αυτά από τη στιγμή που ο πελάτης υπηρεσιών cloud αναθέσει πράξεις επεξεργασίας σε υπηρεσίες cloud, χαρακτηρίζεται ο ίδιος υπεύθυνος επεξεργασίας με την αντίστοιχη ευθύνη τήρησης του κανονιστικού πλαισίου για την προστασία δεδομένων[13]. Ακολούθως πρέπει να τονιστεί ότι η προαναφερόμενη ανισορροπία διαπραγματευτικής ισχύος μεταξύ του παρόχου Υπηρεσιών Υπολογιστικού Νέφους και του πελάτη «δεν συνιστά δικαιολογία ώστε οι πελάτες να αποδέχονται όρους που δεν συμμορφώνονται με τη νομοθεσία περί προστασίας προσωπικών δεδομένων»[14],[15]. Για τον σκοπό αυτό, η ομάδα εργασίας του άρθρου 29 της Οδηγίας 95/46/ΕΚ παρέχει έναν κατάλογο θεμάτων που πρέπει να αντιμετωπίζονται, ώστε να προστατεύονται επαρκώς τα δεδομένα προσωπικού χαρακτήρα[16].

[11] Λίλιαν Μήτρου, Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 4/2015, Οκτώβριος - Νοέμβριος – Δεκέμβριος 2015, σελ.539, υποσημείωση 46.

[12] Γνώμη 1/2010 Ομάδας Άρθρου 29 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», σελ.33, 16-2-2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

[13] Λίλιαν Μήτρου, Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 4/2015, Οκτώβριος - Νοέμβριος – Δεκέμβριος 2015, σελ.539 επ.

[14] S. Ahmed, Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 6/2014, Ιούνιος 2014.

[15] Γνώμη 5/2012 Ομάδας ΄Αρθρου 29 σχετικά με τη νεφοϋπολογιστική, σελ.12-14, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation /files/2012 /wp196_en. pdf

[16] Γνώμη 1/2010 Ομάδας Άρθρου 29 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», σελ.33, 16-2-2010, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

«Η σύμβαση πρέπει, κατ' ελάχιστον, να προβλέπει συγκεκριμένα ότι ο εκτελών την επεξεργασία οφείλει να τηρεί τις οδηγίες του υπεύθυνου της επεξεργασίας και να εφαρμόζει τεχνικά και οργανωτικά μέτρα με γνώμονα την επαρκή προστασία των δεδομένων προσωπικού χαρακτήρα. Για να διασφαλιστεί η ασφάλεια δικαίου, η σύμβαση θα πρέπει επίσης να θέτει τα ακόλουθα ζητήματα:

1. Αναλυτικές πληροφορίες (έκταση και λεπτομέρειες) για τις οδηγίες που πρόκειται να δίνει ο πελάτης στον πάροχο, με ιδιαίτερη έμφαση στις ισχύουσες συμφωνίες επιπέδου εξυπηρέτησης (οι οποίες προτείνεται να είναι αντικειμενικές και μετρήσιμες) και στις συναφείς κυρώσεις (οικονομικές ή άλλες, συμπεριλαμβανομένης της δυνατότητας προσφυγής στη δικαιοσύνη εναντίον του παρόχου σε περίπτωση μη συμμόρφωσης).

2. Προσδιορισμός των μέτρων ασφαλείας προς τα οποία πρέπει να συμμορφώνεται ο πάροχος υπηρεσιών νεφοϋπολογιστικής, αναλόγως κάθε φορά των κινδύνων που ενέχει η επεξεργασία και της φύσης των δεδομένων που χρήζουν προστασίας. Ιδιαίτερης σημασίας κρίνεται ο καθορισμός συγκεκριμένων τεχνικών και οργανωτικών μέτρων, υπό την επιφύλαξη πάντοτε της εφαρμογής αυστηρότερων μέτρων, εάν υπάρχουν, τα οποία δύναται να προβλέπει το εθνικό δίκαιο του πελάτη.

3. Το αντικείμενο και το χρονοδιάγραμμα της υπηρεσίας νεφοϋπολογιστικής που πρόκειται να προσφέρει ο πάροχος υπηρεσιών νεφοϋπολογιστικής, την έκταση, τον τρόπο και τον σκοπό της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τον πάροχο υπηρεσιών νεφοϋπολογιστικής, καθώς και τις κατηγορίες των δεδομένων προσωπικού χαρακτήρα που υφίστανται επεξεργασία.

4. Προσδιορισμός των προϋποθέσεων επιστροφής των δεδομένων (προσωπικού χαρακτήρα) ή καταστροφής τους μόλις ολοκληρωθεί η παροχή της υπηρεσίας. Ακόμη, πρέπει να υπάρχει μέριμνα για την ασφαλή διαγραφή των δεδομένων προσωπικού χαρακτήρα κατόπιν αιτήματος του πελάτη υπηρεσιών νεφοϋπολογιστικής.

5. Συμπερίληψη ρήτρας εμπιστευτικότητας, που θα είναι δεσμευτική για τον πάροχο υπηρεσιών νεφοϋπολογιστικής και για όσους υπαλλήλους του έχουν

ενδεχομένως πρόσβαση στα δεδομένα. Η πρόσβαση στα δεδομένα πρέπει να επιτρέπεται μόνο σε όσους έχουν σχετική άδεια.

6. Υποχρέωση του παρόχου να παρέχει στήριξη στον πελάτη όσον αφορά τη διευκόλυνση της άσκησης των δικαιωμάτων που έχουν τα πρόσωπα στα οποία αναφέρονται τα δεδομένα, και συγκεκριμένα των δικαιωμάτων της πρόσβασης στα δεδομένα και της διόρθωσης ή της διαγραφής τους.

7. Στη σύμβαση προτείνεται να αναφέρεται ρητά ότι ο πάροχος υπηρεσιών νεφοϋπολογιστικής δεν δύναται να κοινοποιεί τα δεδομένα σε τρίτους, ακόμη και για σκοπούς διατήρησης, εκτός και αν προβλέπεται στη σύμβαση ύπαρξη υπεργολάβων. Προτείνεται να αναφέρεται ρητώς στη σύμβαση ότι η πρόσληψη υπό-εκτελούντων την επεξεργασία είναι δυνατή μόνο βάσει συγκατάθεσης η οποία μπορεί γενικώς να δίδεται από τον υπεύθυνο της επεξεργασίας σε συνδυασμό με τη σαφή υποχρέωση του εκτελούντος την επεξεργασία να ενημερώνει τον υπεύθυνο της επεξεργασίας για τυχόν σκοπούμενες συναφείς αλλαγές, με τον δε υπεύθυνο της επεξεργασίας να διατηρεί πάντοτε τη δυνατότητα να αντιταχθεί στις αλλαγές αυτές ή να τερματίσει τη σύμβαση. Ο πάροχος υπηρεσιών νεφοϋπολογιστικής προτείνεται να βαρύνεται με τη σαφή υποχρέωση να κοινοποιεί τα ονόματα όλων των υπεργολάβων που προσλαμβάνει (π.χ. σε δημόσιο ψηφιακό μητρώο). Πρέπει να διασφαλίζεται ότι οι συμβάσεις μεταξύ παρόχου υπηρεσιών νεφοϋπολογιστικής και υπεργολάβου αντικατοπτρίζουν τις διατάξεις της σύμβασης ανάμεσα στον πελάτη και στον πάροχο υπηρεσιών νεφοϋπολογιστικής (δηλαδή οι υπό-εκτελούντες την επεξεργασία πρέπει να βαρύνονται με τις ίδιες ακριβώς συμβατικές υποχρεώσεις που βαρύνουν τον πάροχο υπηρεσιών νεφοϋπολογιστικής). Πρέπει να διασφαλίζεται, συγκεκριμένα, ότι ο πάροχος υπηρεσιών νεφοϋπολογιστικής και όλοι οι υπεργολάβοι ενεργούν αποκλειστικά και μόνο βάσει των οδηγιών του πελάτη υπηρεσιών νεφοϋπολογιστικής. Όπως διευκρινίζεται στο κεφάλαιο για την υπό-εκτέλεση της επεξεργασίας, προτείνεται να καθορίζονται με σαφήνεια στη σύμβαση οι αλυσιδωτές ευθύνες. Προτείνεται να προβλέπεται η υποχρέωση του εκτελούντος την επεξεργασία να οριοθετεί τις διαδικασίες διεθνούς διαβίβασης δεδομένων, π.χ. υπογράφοντας συμβάσεις με τους υπό-εκτελούντες την επεξεργασία, έχοντας ως βάση τις τυποποιημένες συμβατικές ρήτρες της απόφασης 2010/87/ΕΕ.

8. Σαφής καθορισμός των ευθυνών του παρόχου υπηρεσιών νεφοϋπολογιστικής όσον αφορά την ενημέρωση του πελάτη υπηρεσιών νεφοϋπολογιστικής σε περίπτωση παραβίασης δεδομένων η οποία θίγει τα δεδομένα του τελευταίου.

9. Υποχρέωση του παρόχου υπηρεσιών νεφοϋπολογιστικής να παρέχει κατάλογο των τοποθεσιών στις οποίες δύναται να γίνεται επεξεργασία των δεδομένων.

10. Το δικαίωμα του υπευθύνου της επεξεργασίας να παρακολουθεί τις διαδικασίες επεξεργασίας του παρόχου υπηρεσιών νεφοϋπολογιστικής και την αντίστοιχη υποχρέωση του τελευταίου να συνεργάζεται.

11. Προτείνεται να καθορίζεται στη σύμβαση ότι ο πάροχος υπηρεσιών νεφοϋπολογιστικής πρέπει να ενημερώνει τον πελάτη για συναφείς αλλαγές που αφορούν την εκάστοτε παρεχόμενη υπηρεσία νεφοϋπολογιστικής όπως, για παράδειγμα, η εκτέλεση πρόσθετων λειτουργιών.

12. Προτείνεται η σύμβαση να προβλέπει την καταγραφή και τον έλεγχο των συναφών διαδικασιών επεξεργασίας δεδομένων προσωπικού χαρακτήρα που επιτελούνται από τον πάροχο υπηρεσιών νεφοϋπολογιστικής ή τους υπεργολάβους.

13. Ενημέρωση του πελάτη υπηρεσιών νεφοϋπολογιστικής σχετικά με κάθε νομικά δεσμευτικό αίτημα κοινοποίησης των δεδομένων προσωπικού χαρακτήρα που υποβάλλεται από αρχή επιβολής του νόμου, εκτός αν υπάρχει σχετική απαγόρευση, όπως απαγόρευση συνοδευόμενη από ποινικές κυρώσεις για τη διατήρηση του εμπιστευτικού χαρακτήρα αστυνομικής έρευνας.

14. Γενική υποχρέωση του παρόχου να παρέχει διαβεβαιώσεις ότι οι ρυθμίσεις οργάνωσης και επεξεργασίας δεδομένων που εφαρμόζει ο ίδιος (όπως και οι αντίστοιχες ρυθμίσεις που εφαρμόζουν οι υπό-εκτελούντες της επεξεργασία τους οποίους έχει ενδεχομένως προσλάβει) συμμορφώνονται προς τις ισχύουσες επιταγές και τα πρότυπα της εθνικής και διεθνούς νομοθεσίας.

Επισημαίνεται ακόμη ότι σε περίπτωση παραβίασης -των αρχών νόμιμης επεξεργασίας προσωπικών δεδομένων- από τον υπεύθυνο της επεξεργασίας, κάθε πρόσωπο που

υπέστη ζημία ως αποτέλεσμα αθέμιτης επεξεργασίας, δικαιούται αποζημίωση από τον υπεύθυνο της επεξεργασίας για την ζημία που υπέστη. Επίσης εξετάζεται η περίπτωση κατά την οποία οι εκτελούντες την επεξεργασία χρησιμοποιούν τα δεδομένα για άλλους σκοπούς ή τα κοινοποιούν ή τα χρησιμοποιούν κατά τρόπο που συνιστά παραβίαση της σύμβασης, τότε θα πρέπει να θεωρούνται κι αυτοί ως υπεύθυνοι της επεξεργασίας και συνεπώς να έχουν την ευθύνη για τις παραβιάσεις στις οποίες συμμετείχαν[17].

Στην περίπτωση του υπολογιστικού νέφους αναπτύσσονται πολύπλοκες και πολυεπίπεδες δομές επεξεργασίας δεδομένων οι οποίες μπορεί να βρίσκονται σε διαφορετικές χώρες και να εκτελούνται από διαφορετικά πρόσωπα, τα οποία είτε αποτελούν παράλληλα εκτελούντες την επεξεργασία ή υποεκτελούντες αυτή. Έτσι γίνεται ιδιαίτερα απαιτητικός ο προσδιορισμός αφενός καθενός των πολλαπλών επιπέδων επεξεργασίας, αφετέρου δε, του εμπλεκόμενου φορέα ως και του ρόλου του σε καθένα από αυτά τα επίπεδα. Ο πελάτης της υπηρεσίας συμβάλλεται μόνο με τον πάροχο του ανώτερου επιπέδου παροχής της υπηρεσίας που λαμβάνει και συνήθως δεν γνωρίζει καν τους παρόχους των λοιπών υπο-επιπέδων και δομών της υπηρεσίας. Κατ' αυτόν τον τρόπο η παροχή μίας υπηρεσίας μπορεί να διαρθρώνεται σε διάφορα επίπεδα και να διαφοροποιείται ο ρόλος του παρόχου ανά επίπεδο. Ένας πάροχος cloud που παρέχει μία πλευρά της υπηρεσίας, για παράδειγμα το λογισμικό, μπορεί να διαφοροποιείται από εκείνον που παρέχει μία άλλη συνισταμένη της ίδιας υπηρεσίας, όπως την πλατφόρμα, τη φιλοξενία (αποθηκευτικό χώρο) ή την τεχνολογική υποδομή. Για παράδειγμα, ένας πάροχος υπηρεσίας κοινωνικής δικτύωσης αποτελεί υπεύθυνο επεξεργασίας για τα δεδομένα (επώνυμο, όνομα, email, ημερομηνία γέννησης, κ.λπ.) τα οποία πρέπει τα φυσικά πρόσωπα που εγγράφονται στην υπηρεσία του να εισάγουν στη φόρμα εγγραφής. Όμως, ως προς τα προσωπικά δεδομένα τα οποία οι χρήστες της υπηρεσίας του «ανεβάζουν» και επεξεργάζονται διαδικτυακά με δική τους απόφαση και πρωτοβουλία αποτελεί εκτελούντα την επεξεργασία[18]. Στην περίπτωση των επιγραμμικών υπηρεσιών κοινωνικής δικτύωσης, οι πάροχοι υπηρεσιών νέφους πρέπει να χαρακτηρίζονται υπεύθυνοι επεξεργασίας δεδομένων, δεδομένου ότι (και στον

[17] Γνώμη 5/2012 Ομάδας ΄Αρθρου 29 σχετικά με τη νεφοϋπολογιστική, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation /files/2012 /wp196_en. pdf

[18] Ευγενία Σμυρνάκη, Υπολογιστικό Νέφος (Cloud) και Προσωπικά Δεδομένα - Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016, Pro Justitia Τόμος 2/2016.

βαθμό που) επεξεργάζονται δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από τη χρήση υπηρεσιών cloud computing για δικούς τους σκοπούς(ή και νέους), όπως σκοπούς μάρκετινγκ ή διαβίβασης σε τρίτους και μόνον για την αντίστοιχη δραστηριότητά τους[19].

Βάσει των ανωτέρω, όταν ο πάροχος cloud προσφέρει τις υπηρεσίες του απευθείας σε τελικούς χρήστες – καταναλωτές, τότε έχει την ιδιότητα του υπευθύνου επεξεργασίας σχετικά με τα προσωπικά δεδομένα που απαιτείται να γνωστοποιήσουν και να δώσουν στον πάροχο οι τελικοί χρήστες προκειμένου να κάνουν χρήση της υπηρεσίας ή με τα προσωπικά δεδομένα που χρησιμοποιεί για διαφημιστικούς σκοπούς, σκοπούς μάρκετινγκ ή διαβίβασης σε τρίτους. Επίσης, κατέχει το ρόλο υπευθύνου επεξεργασίας των συλλεγόμενων μεταδεδομένων που αφορούν στην χρήση της υπηρεσίας από τον πελάτη (όπως για παράδειγμα, επιγραμμικά αναγνωριστικά ταυτότητας, διεύθυνση IP, ώρα εισόδου στην υπηρεσία, διάρκεια παραμονής κ.λπ.). Ενώ όταν ο πελάτης υπηρεσιών cloud είναι ο υπεύθυνος επεξεργασίας προσωπικών δεδομένων στο πλαίσιο της υπηρεσίας υπολογιστικού νέφους που κάνει χρήση, τότε τα πρόσωπα (φυσικά ή νομικά) που κατέχουν κάποιο ρόλο στην επεξεργασία των εν λόγω δεδομένων για λογαριασμό του αποτελούν εκτελούντες την επεξεργασία όπως εν προκειμένω οι πάροχοι υπηρεσιών cloud. Ο υπεύθυνος επεξεργασίας συμβάλλεται συνήθως μόνο με τον πάροχο της τελικής εφαρμογής της οποίας κάνει χρήση.

2.6 Υποχρεώσεις υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία

Ο προσδιορισμός των ρόλων συνεπάγεται απαιτήσεις και υποχρεώσεις και για τους υπευθύνους επεξεργασίας άλλα και για τους εκτελούντες την επεξεργασία. Ο υπεύθυνος επεξεργασίας οφείλει να λάβει κάθε αναγκαίο μέτρο, ώστε να διασφαλίσει την προστασία των δεδομένων από τον εκτελούντα την επεξεργασία. Ο υπεύθυνος επεξεργασίας, δηλαδή ο πελάτης υπηρεσιών νέφους, οφείλει να διασφαλίζει

[19] Λίλιαν Μήτρου, Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, Νομική Βιλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 4/2015, Οκτώβριος - Νοέμβριος – Δεκέμβριος 2015, σελ.540 επ.

πραγματικό έλεγχο επί του εκτελούντος την επεξεργασία των δεδομένων σε ολόκληρη την αλυσίδα ανάθεσης, ο δε εκτελών την επεξεργασία των δεδομένων οφείλει να εξασφαλίζει τη διαφάνεια έναντι του υπευθύνου επεξεργασίας και να παρέχει εγγυήσεις, όσον αφορά την καταγραφή και τον έλεγχο των συναφών διαδικασιών επεξεργασίας προσωπικών δεδομένων[20,21].

Σύμφωνα με το άρθρο 28 παρ. 1 του ΓΚΠΔ προβλέπεται ότι ο υπεύθυνος επεξεργασίας χρησιμοποιεί μόνο εκτελούντες την επεξεργασία που παρέχουν επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε η επεξεργασία να πληροί τις απαιτήσεις του Κανονισμού. Η τήρηση εγκεκριμένου κώδικα δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης από τον εκτελούντα την επεξεργασία αποτελούν δύο εκ των κριτηρίων που λαμβάνονται υπόψη για την κρίση περί της παροχής επαρκών διαβεβαιώσεων (άρθρο 28 παρ. 5 ΓΚΠΔ). Αναγνωρίζεται ο σημαντικός ρόλος που έχει ο εκτελών την επεξεργασία στο βαθμό συμμόρφωσης του υπεύθυνου επεξεργασίας με τις επιταγές και απαιτήσεις του Κανονισμού.

Σύμφωνα με το άρθρο 28 παρ. 3 ΓΚΠΔ η ανάθεση της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα από τον υπεύθυνο επεξεργασίας στον εκτελούντα την επεξεργασία πρέπει να γίνεται μόνον βάσει σύμβασης ή άλλης νομικής πράξης βάσει καταγεγραμμένων εντολών του υπεύθυνου επεξεργασίας. Ενώ στην περίπτωση υπεργολαβίας (sub-contracting), όταν δηλαδή ο εκτελών την επεξεργασία προσλαμβάνει άλλο εκτελούντα, τότε οι ίδιες υποχρεώσεις πρέπει να επιβληθούν και στον υπεργολάβο εκτελούντα την επεξεργασία μέσω σύμβασης (back-to-back contract). Εάν δε, ο υπο-εκτελών την επεξεργασία αδυνατεί να ανταποκριθεί στις υποχρεώσεις του Κανονισμού, ο αρχικός εκτελών την επεξεργασία παραμένει πλήρως υπεύθυνος έναντι του υπευθύνου επεξεργασίας για την τήρηση των διατάξεων του Κανονισμού (άρθρο 28 παρ.4 ΓΚΠΔ). Σε κάθε δε περίπτωση ο εκτελών την επεξεργασία δεν προσλαμβάνει άλλον εκτελούντα χωρίς προηγούμενη ειδική ή γενική άδεια του υπευθύνου επεξεργασίας (άρθρο 28 παρ.2 ΓΚΠΔ). Αν υπάρξει παραβίαση

[20] Λίλιαν Μήτρου, Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, Νομική Βιλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 4/2015, Οκτώβριος - Νοέμβριος – Δεκέμβριος 2015, σελ.534 επ.
[21] Γνώμη 5/2012 Ομάδας ΄Αρθρου 29 σχετικά με τη νεφοϋπολογιστική.

δεδομένων προσωπικού χαρακτήρα ο εκτελών την επεξεργασία ενημερώνει αμελλητί τον υπεύθυνο επεξεργασίας (άρθρο 32 παρ.1 ΓΚΠΔ).

Μια ακόμη σημαντική υποχρέωση τόσο του υπευθύνου επεξεργασίας όσο και του εκτελούντος την επεξεργασία είναι η υποχρέωση ασφάλειας των δεδομένων μέσω κατάλληλων τεχνικών και οργανωτικών μέτρων (άρθρο 33 παρ.2 ΓΚΠΔ).

Όσον αφορά τις διαβιβάσεις σε τρίτες χώρες έχει προβλεφθεί στο άρθρο 46 του ΓΚΠΔ ότι μπορούν να πραγματοποιηθούν αν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία έχουν παράσχει κατάλληλες εγγυήσεις, μεταξύ άλλων τυποποιημένες ρήτρες προστασίας δεδομένων (standard data protection clauses) ή εγκεκριμένους κώδικες δεοντολογίας ή εγκεκριμένο μηχανισμό πιστοποίησης (certication mechanism).

Προβλέπεται πλέον ρητώς το δικαίωμα διαγραφής (δικαίωμα στη λήθη) των δεδομένων του υποκειμένου από τον υπεύθυνο επεξεργασίας και μάλιστα χωρίς αδικαιολόγητη καθυστέρηση (άρθρο 17 ΓΚΠΔ). Η εν λόγω υποχρέωση αφορά μόνο στον υπεύθυνο επεξεργασίας αλλά καθίσταται σαφές ότι αφορά άμεσα και επηρεάζει τον εκτελούντα με τεχνικά και αυτοματοποιημένα μέσα πάροχο υπηρεσίας cloud. Ο υπεύθυνος επεξεργασίας θα μετακυλίσει στον πάροχο υπηρεσίας cloud το σχετικό αίτημα του τελικού χρήστη ως και την υλοποίηση της αντίστοιχης υποχρέωσης πλήρους διαγραφής των δεδομένων του υποκειμένου. Ζήτημα ωστόσο αποτελεί εάν και κατά πόσο θα μπορεί να υλοποιηθεί η πλήρης διαγραφή από τον εκτελούντα την επεξεργασία πάροχο του νέφους, δεδομένου ότι αμφισβητείται η δυνατότητα πλήρους διαγραφής όλων των δεδομένων και των αντιγράφων τους που έχουν δημιουργηθεί.

Ένα ακόμη σημαντικό δικαίωμα του υποκειμένου των προσωπικών δεδομένων είναι η φορητότητα των δεδομένων (άρθρο 20 ΓΚΠΔ), κατά το οποίο το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, και τα οποία έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα μορφότυπο (data portability) και να ζητάει απευθείας διαβίβαση των προσωπικών του δεδομένων από τον ένα υπεύθυνο επεξεργασίας στον άλλο, εφόσον η επεξεργασία βασίζεται είτε στη συγκατάθεσή του είτε σε σύμβαση. Το δικαίωμα στη φορητότητα των δεδομένων αφενός διευκολύνει

την ενάσκηση του δικαιώματος πρόσβασης και αφετέρου ενδυναμώνει τη θέση του καταναλωτή έναντι πρακτικών εγκλωβισμού – κλειδώματος δεδομένων (lock-in). Για παράδειγμα, θα μπορεί πλέον το υποκείμενο να ζητήσει την λήψη της λίστας των επαφών του ηλεκτρονικού του ταχυδρομείου και να τη μεταφέρει σε κάποιον άλλο πάροχο ή πλατφόρμα. Για να διασφαλιστεί η ενάσκηση του δικαιώματος αυτού ένας νομικός σύμβουλος θα πρέπει να διαπραγματεύεται και να λαμβάνει γραπτές δεσμεύσεις ότι ο πάροχος Υπηρεσιών Υπολογιστικού Νέφους δεν αποκτά κανένα δικαίωμα ιδιοκτησίας επί των δεδομένων των πελατών του. Είναι, επίσης, σημαντικό να διασφαλίζεται ότι ο πάροχος Υπηρεσιών Υπολογιστικού Νέφους θα διαγράφει μόνιμα τα δεδομένα του πελάτη του, κατόπιν αιτήματός του, μέσα σε εύλογο χρονικό διάστημα, για την πρόληψη ζητημάτων εμπιστευτικότητας[22].

3 Πεδίο εφαρμογής Γενικού Κανονισμού Προστασίας Δεδομένων

Ο Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016 τέθηκε σε εφαρμογή στις 25/5/2018 και σύμφωνα με το άρθρο 3 παρ.1 «ο κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων ενός υπεύθυνου επεξεργασίας ή εκτελούντος την επεξεργασία που είναι εγκατεστημένος στην Ένωση, ανεξάρτητα από το κατά πόσο η επεξεργασία πραγματοποιείται εντός Ε.Ε.». Στην κατεύθυνση αυτή έχει εκδοθεί και ο ελληνικός Νόμος 4624/2019 για την εφαρμογή του ΓΚΠΔ.

Ριζική διεύρυνση του πεδίου εφαρμογής του Κανονισμού εισάγεται με το άρθρο 3 παρ.2 εδ. α΄ και β΄, όπου ορίζεται ότι «ο κανονισμός εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων που βρίσκονται στην Ένωση από υπεύθυνο ή εκτελούντα την επεξεργασία μη εγκατεστημένο στην Ένωση, εάν οι δραστηριότητες επεξεργασίας σχετίζονται με: α) την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα δεδομένων εντός της Ένωσης, ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων, ή β) με την παρακολούθηση της

[22] S. Ahmed, Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 6/2014, Ιούνιος 2014.

συμπεριφοράς τους. Στο βαθμό που η συμπεριφορά αυτή λαβαίνει χώρα εντός της Ένωσης».

Ως προς την προσφορά αγαθών και υπηρεσιών και μάλιστα ανεξάρτητα από την ύπαρξη αμοιβής, πρέπει να σημειωθεί ότι παρά την ευρύτητα της διατύπωσης δεν ήταν σκοπός του νομοθέτη ο Κανονισμός να εφαρμοστεί στο σύνολο του Διαδικτύου. Σύμφωνα με την Αιτιολογική Σκέψη 23 παραθέτονται κριτήρια για τη διαπίστωση της παροχής αγαθών και υπηρεσιών, όπως η χρήση γλώσσας ή νομίσματος που χρησιμοποιούνται σε ένα ή περισσότερα κράτη, με δυνατότητα παραγγελίας προϊόντων και υπηρεσιών σε αυτή την άλλη γλώσσα, ή η αναφορά σε πελάτες ή χρήστες που βρίσκονται στην ΄Ενωση.

Ως προς την παρακολούθηση της συμπεριφοράς, προκειμένου για την εφαρμογή του Κανονισμού κρίσιμη είναι τελικά η φυσική/γεωγραφική θέση του χρήστη, αν και η αντίστοιχη ρύθμιση σχετίζεται με online συμπεριφορά- συμπεριφορά στο διαδίκτυο. Εκτός από την πιθανή- ενδεχόμενη δυσκολία στον προσδιορισμό της γεωγραφικής θέσης μιας διαδικτυακής διεύθυνσης (IP adress), προβληματίζει το αν ο όρος «συμπεριφορά» είναι πλέον δόκιμος για να αποδόσει τη διαδικτυακή συμπεριφορά κάποιου[23]. Είναι εμφανές ότι όταν ο νομοθέτης αναφέρεται στο online tracking είχε υπόψιν του τη συμπεριφορική στοχευμένη διαδικτυακή διαφήμιση. Κάτι τέτοιο φαίνεται να στηρίζεται και στην Αιτιολογική Σκέψη 24 του ΓΚΠΔ, η οποία αναφέρει ότι η παρακολούθηση περιλαμβάνει ενδεικτικά τη «δυνητική μετέπειτα χρήση τεχνικών επεξεργασίας δεδομένων προσωπικού χαρακτήρα οι οποίες συνίστανται στη διαμόρφωση του «προφίλ» ενός φυσικού προσώπου, ιδίως με σκοπό να ληφθούν αποφάσεις που το αφορούν ή να αναλυθούν ή να προβλεφθούν οι προσωπικές προτιμήσεις, οι συμπεριφορές και οι νοοτροπίες του». Ενώ στην αιτιολογική σκέψη 30 αναφέρεται ότι συσκευές, εφαρμογές, εργαλεία και πρωτόκολλα αυτών, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία, όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων, αποτελούν στοιχεία που συλλέγονται αναφορικά με φυσικά πρόσωπα και συνδυαζόμενα με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες

[23] Μήτρου Λ., 2017, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων¸ νέο δίκαιο, νέες υποχρεώσεις, νέα δικαιώματα, εκδόσεις Σάκκουλα, σελ. 53.

πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για τη δημιουργία προφίλ των φυσικών προσώπων και να οδηγήσουν στην αναγνώριση της ταυτότητάς τους.

Παρατηρείται λοιπόν μία σαφής πρόθεση του Ευρωπαίου Νομοθέτη να διευρύνει το πεδίο εφαρμογής της νομοθεσίας για την προστασία δεδομένων προσωπικού χαρακτήρα και να την αποδεσμεύσει από τον τόπο όπου τα δεδομένα αποθηκεύονται ή επεξεργάζονται. Μηχανές αναζήτησης, πλατφόρμες ψηφιακών κοινωνικών δικτύων και πάροχοι υπηρεσιών νέφους συμπεριλαμβάνονται στις ρυθμίσεις για την προστασία προσωπικών δεδομένων με τη διεύρυνση του πεδίου εφαρμογής, ως μία ρεαλιστική προσέγγιση και επιλογή του Ευρωπαίου νομοθέτη[24].

Αντικείμενο της επιχειρούμενης με τον ΓΚΠΔ ρύθμισης είναι οι συμπεριφορές, πράξεις ή παραλείψεις, των εμπλεκομένων προσώπων που διενεργούν ή υποστηρίζουν επικοινωνίες και συναλλαγές που ή έχουν ως προϋπόθεση ή που παράγουν προσωπική πληροφορία[25]. Μέσα σ' αυτό το πλαίσιο του ΓΚΠΔ θα 'ναι δυσκολότερο να παρακαμφθεί η εφαρμογή των διατάξεών του και ίσως έτσι να 'ναι αποτελεσματικότερη η επιδιωκόμενη προστασία των προσωπικών δεδομένων.

Στην περίπτωση που εφαρμόζεται το άρθρο 3 παρ.2, όπως ανωτέρω αναφέρεται, το άρθρο 27 του ΓΚΠΔ προβλέπει μια επιπλέον υποχρέωση για τον υπεύθυνο επεξεργασίας ή για τον εκτελούντα την επεξεργασία που δεν είναι εγκατεστημένος στην Ένωση, την υποχρέωση ορισμού γραπτώς εκπροσώπου που είναι εγκατεστημένος σε ένα από τα κράτη μέλη όπου βρίσκονται τα υποκείμενα των δεδομένων των οποίων τα δεδομένα υφίστανται επεξεργασία σε σχέση με προσφορά αγαθών ή υπηρεσιών προς αυτά ή των οποίων η συμπεριφορά παρακολουθείται. Στον εκπρόσωπο θα απευθύνονται οι εποπτικές αρχές και τα υποκείμενα των δεδομένων, επιπρόσθετα ή αντί του υπεύθυνου ή εκτελούντος την επεξεργασία, για όλα τα θέματα που σχετίζονται με την επεξεργασία. Η υποχρέωση αυτή δεν υφίσταται εάν η

[24] Μήτρου Λ., 2017, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων¸ νέο δίκαιο, νέες υποχρεώσεις, νέα δικαιώματα, εκδόσεις Σάκκουλα, σελ. 53.

[25] Βλ. ανωτέρω υποσημείωση 24.

επεξεργασία που είναι περιστασιακή, δεν περιλαμβάνει, σε μεγάλο βαθμό, επεξεργασία ειδικών κατηγοριών δεδομένων ή επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα και δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[26]. Παράγοντες που λαμβάνονται υπόψη για την εφαρμογή της ως άνω εξαίρεσης είναι η φύση, το πλαίσιο, το πεδίο εφαρμογής και οι σκοποί της επεξεργασίας. Στη διάταξη αυτή δεν παρέχονται από τον ΓΚΠΔ συγκεκριμένα στοιχεία για τον προσδιορισμό της συχνότητας της επεξεργασίας που θα την κατέτασσε στην κατηγορία της «περιστασιακής» αλλά και πώς προσδιορίζεται ποσοτικά ή και ποιοτικά η έννοια της «μεγάλης κλίμακας» στην επεξεργασία ειδικών κατηγοριών δεδομένων. Εν προκειμένω η εφαρμογή της εξαίρεσης του ως άνω άρθρου σε παρόχους υπηρεσιών υπολογιστικού νέφους διαφαίνεται δυσχερής. Τα τεχνικά και λειτουργικά χαρακτηριστικά των παρόχων υπηρεσιών υπολογιστικού νέφους, ιδίως δε ο μεγάλος αριθμός των πελατών τους (φυσικών ή νομικών προσώπων), το γεγονός ότι δεν υπάρχει γνώση και έλεγχος του είδους των δεδομένων που υφίστανται επεξεργασία μέσω των συστημάτων τους, ούτε δέσμευση ή περιορισμός εκ των προτέρων του πελάτη για το είδος των δεδομένων που θα επεξεργαστεί, αναδεικνύουν την εκτίμηση ότι θα ’ναι δύσκολο να εμπίπτουν στην εφαρμογή αυτής της εξαίρεσης οι πάροχοι υπηρεσιών cloud και έτσι θα υποχρεούνται στον ορισμό εκπροσώπου. Η επεξεργασία εν γένει των προσωπικών δεδομένων είναι απόρρητη και πρέπει να θωρακίζεται με αυστηρούς μηχανισμούς ασφάλειας, φυσικής ή ηλεκτρονικής.

3.1 Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων

Ο ΓΚΠΔ σύστησε το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (εφεξής ΕΣΠΔ) ως όργανο της ΕΕ με νομική προσωπικότητα[27]. Είναι ο διάδοχος της Ομάδας εργασίας του άρθρου 29, η οποία είχε συσταθεί δυνάμει της Οδηγίας 95/46/ΕΚ για την Προστασία Δεδομένων με σκοπό να συμβουλεύει την Επιτροπή σχετικά με μέτρα της ΕΕ που επηρεάζουν τα δικαιώματα των φυσικών προσώπων ως προς την επεξεργασία δεδομένων προσωπικού χαρακτήρα και την ιδιωτική ζωή, να προάγει την ομοιόμορφη εφαρμογή της οδηγίας και να παρέχει γνώμες εμπειρογνώμονα στην Επιτροπή σε

[26] ΓΚΠΔ άρθρο 27 παρ. 2 εδάφιο α΄.
[27] ΓΚΠΔ άρθρο 68.

θέματα σχετικά με την προστασία δεδομένων. Η Ομάδα εργασίας του άρθρου 29 απαρτιζόταν από εκπροσώπους των εποπτικών αρχών των κρατών μελών της ΕΕ, καθώς και εκπροσώπους της Επιτροπής και του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ). Το ΕΣΠΔ είναι ένας ανεξάρτητος ευρωπαϊκός οργανισμός, ο οποίος συμβάλλει στη συνεκτική εφαρμογή των κανόνων προστασίας δεδομένων σε ολόκληρη την Ευρωπαϊκή Ένωση και προάγει τη συνεργασία μεταξύ των αρχών προστασίας δεδομένων της ΕΕ. Το ΕΣΠΔ απαρτίζεται από τους προϊσταμένους των εποπτικών αρχών και από τον Ευρωπαίο Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ) ή τους εκπροσώπους τους. Αντί να απαντά σε συγκεκριμένα μεμονωμένα αιτήματα, το ΕΣΠΔ εκδίδει γενικές κατευθυντήριες γραμμές. Έχει τη δυνατότητα[28]:

- να παρέχει γενική καθοδήγηση (συμπεριλαμβανομένων κατευθυντήριων αρχών, συστάσεων και βέλτιστων πρακτικών) για την αποσαφήνιση της νομοθεσίας
- να παρέχει συμβουλές στην Ευρωπαϊκή Επιτροπή σχετικά με οποιοδήποτε θέμα αφορά την προστασία δεδομένων προσωπικού χαρακτήρα και τις νέες προτάσεις νομοθεσίας στην Ευρωπαϊκή Ένωση·
- να εκδίδει πορίσματα συνεκτικότητας σε διασυνοριακές υποθέσεις προστασίας δεδομένων· και
- να προωθεί τη συνεργασία και την αποτελεσματική ανταλλαγή πληροφοριών και βέλτιστων πρακτικών μεταξύ των εθνικών εποπτικών αρχών.

Εκδίδει επίσης ετήσια έκθεση σχετικά με τις δραστηριότητές του, η οποία δημοσιεύεται και διαβιβάζεται στο Ευρωπαϊκό Κοινοβούλιο, στο Συμβούλιο και στην Επιτροπή[29,30].

[28] https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_el

[29] «Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων - Έκδοση 2018», Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, 2019, σελ. 250, https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_el.pdf

[30] Βλ. ανωτέρω υποσημείωση 28

4 Διασυνοριακές ροές δεδομένων

Πριν τη θέσπιση του Γενικού Κανονισμού Προστασίας Δεδομένων 679/2016 οι διασυνοριακές ροές προσωπικών δεδομένων επιτρεπόταν βάσει του άρθρου 25 της Οδηγίας 95/46/ΕΚ, όπως ενσωματώθηκε στην Ελλάδα με το Ν. 2472/1997.Συγκεκριμένα βάσει του άρθρου 9 παρ.1 του Ν. 2472/1997:

«1. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα είναι ελεύθερη: α) προς χώρες μέλη της Ευρωπαϊκής Ένωσης,
β) προς χώρα μη μέλος της Ευρωπαϊκής Ένωσης, μετά από άδεια της Αρχής που παρέχεται εάν κρίνει ότι η εν λόγω χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας. Προς τούτο, λαμβάνει υπόψη ιδίως τη φύση των δεδομένων, τους σκοπούς και τη διάρκεια της επεξεργασίας, τους σχετικούς γενικούς και ειδικούς κανόνες δικαίου, τους κώδικες δεοντολογίας, τα μέτρα ασφαλείας για την προστασία δεδομένων προσωπικού χαρακτήρα, καθώς και το επίπεδο προστασίας των χωρών προέλευσης, διέλευσης και τελικού προορισμού των δεδομένων. Δεν απαιτείται άδεια της Αρχής εφόσον η Ευρωπαϊκή Επιτροπή έχει αποφανθεί, με τη διαδικασία του άρθρου 31 παρ. 2 της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 24ης Οκτωβρίου 1995, ότι η χώρα αυτή εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, κατά την έννοια της παρ. 2 του άρθρου 25 της ανωτέρω Οδηγίας.» (όπως τροποποιήθηκε με την παρ.1 του άρθρου 24 του Ν.3471/2006).

«2. Η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς χώρα που δεν ανήκει στην Ευρωπαϊκή Ένωση και η οποία δεν εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, επιτρέπεται κατ` εξαίρεση, με άδεια της Αρχής, εφόσον συντρέχει μία ή περισσότερες από τις κατωτέρω προϋποθέσεις:
α) Το υποκείμενο των δεδομένων έδωσε τη συγκατάθεσή του για τη διαβίβαση, εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που να αντίκειται στο νόμο ή τα χρηστά ήθη.
β)Η διαβίβαση είναι απαραίτητη: i) για τη διασφάλιση ζωτικού συμφέροντος του υποκειμένου των δεδομένων, εφόσον αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του, ή "ii). για τη συνομολόγηση και εκτέλεση σύμβασης μεταξύ αυτού και του υπευθύνου επεξεργασίας ή μεταξύ του υπευθύνου επεξεργασίας

και τρίτου προς το συμφέρον του υποκειμένου των δεδομένων.» (όπως τροποποιήθηκε με την παρ.2 του άρθρου 24 του Ν.3471/2006 (ΦΕΚ Α 133/2006))

«γ) Η διαβίβαση είναι απαραίτητη για την αντιμετώπιση εξαιρετικής ανάγκης και τη διαφύλαξη υπέρτερου δημόσιου συμφέροντος, ιδίως για την εκτέλεση συμβάσεων συνεργασίας με δημόσιες Αρχές της άλλης χώρας, εφόσον ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία της ιδιωτικής ζωής και των θεμελιωδών ελευθεριών και την άσκηση των σχετικών δικαιωμάτων.

δ) Η διαβίβαση είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον του δικαστηρίου.

ε) Η μετάδοση πραγματοποιείται από δημόσιο μητρώο, το οποίο κατά το νόμο προορίζεται για την παροχή πληροφοριών στο κοινό και είναι προσιτό στο κοινό ή σε κάθε πρόσωπο που αποδεικνύει έννομο συμφέρον, εφόσον στη συγκεκριμένη περίπτωση πληρούνται οι νόμιμες προϋποθέσεις για την πρόσβαση στο μητρώο.

στ) Ο υπεύθυνος επεξεργασίας παρέχει επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων των υποκειμένων και την άσκηση των σχετικών δικαιωμάτων τους, όταν οι εγγυήσεις προκύπτουν από συμβατικές ρήτρες, σύμφωνες με τις ρυθμίσεις του παρόντος νόμου. Δεν απαιτείται άδεια εάν η Ευρωπαϊκή Επιτροπή έκρινε, κατά το άρθρο 26 παρ. 4 της Οδηγίας 95/46/ΕΚ, ότι ορισμένες συμβατικές ρήτρες παρέχουν επαρκείς εγγυήσεις για την προστασία των προσωπικών δεδομένων.» (όπως η περ. στ΄ προστέθηκε με την παρ.3 του άρθρου 24 του Ν.3471/2006).

Οι κανόνες της ΕΕ για την προστασία των δεδομένων ισχύουν για τον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ), ο οποίος περιλαμβάνει όλες τις χώρες της ΕΕ και χώρες εκτός ΕΕ, την Ισλανδία, το Λιχτενστάιν και τη Νορβηγία. Συνεπώς η διαβίβαση προσωπικών δεδομένων από χώρες της Ε.Ε. αναφέρεται στις χώρες που ανήκουν στον Ευρωπαϊκό Οικονομικό Χώρο (ΕΟΧ), ο οποίος περιλαμβάνει όλες τις χώρες της ΕΕ και χώρες εκτός ΕΕ, την Ισλανδία, το Λιχτενστάιν και τη Νορβηγία[31].

4.1 Αρχές του Ασφαλούς Λιμένα (Safe Harbour Principles)

Πολλοί πάροχοι υπηρεσιών νέφους και μηχανές αναζήτησης έχουν προσχωρήσει οικειοθελώς στις Αρχές του Ασφαλούς Λιμένα (Safe Harbour Principles), δηλ. το

[31] Ευγενία Αλεξανδροπούλου – Αιγυπτιάδου, Προσωπικά Δεδομένα, 2016, εκδόσεις Νομική Βιβλιοθήκη, σελ.120, υποσημείωση 295.

σύνολο αρχών/κανόνων που εξέδωσε το Υπουργείο Εμπορίου των ΗΠΑ και δεσμεύονται να τηρούν οι περιλαμβανόμενες σε σχετικό κατάλογο αμερικάνικες επιχειρήσεις, με στόχο τη διευκόλυνση της διαβίβασης δεδομένων από την Ε.Ε. σε εταιρείες εγκατεστημένες στις ΗΠΑ, το οποίο η Ευρωπαϊκή Επιτροπή ενέκρινε το 2000 με την απόφαση 2000/520 της Επιτροπής βάσει της Οδηγίας 95/46/ΕΚ .

Για να εξάγει μια οντότητα που υπόκειται στους κανονισμούς απορρήτου της ΕΕ δεδομένα προσωπικού χαρακτήρα σε προορισμό που υπόκειται στη νομοθεσία των ΗΠΑ, πρέπει η ευρωπαϊκή οντότητα να διασφαλίσει ότι η οντότητα λήψης παρέχει επαρκείς διασφαλίσεις για την προστασία αυτών των δεδομένων από μια σειρά ατυχημάτων. Συνεπώς η προσχώρηση στους κανόνες Ασφαλούς λιμένος είναι μια εθελοντική αυτοπιστοποίηση. Ο εθελοντικός χαρακτήρας είναι σχετικός, καθώς ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να συμμορφώνεται με τους κανονισμούς της ΕΕ για την προστασία της ιδιωτικής ζωής, αλλά υπάρχουν εναλλακτικές μέθοδοι συμμόρφωσης (όπως οι πρότυπες ρήτρες)[32].Εάν επιλεγεί σαν τρόπος συμμόρφωσης η ένταξη στο Safe Harbor, η οντότητα πρέπει να αυτοπιστοποιήσει τη συμμόρφωσή της με τις λεγόμενες Αρχές Ασφαλούς Λιμένα, και ο υπεύθυνος επεξεργασίας δεδομένων που εξάγει τα δεδομένα πρέπει να επαληθεύσει ότι ο προορισμός των ΗΠΑ είναι πράγματι στη λίστα Safe Harbor.

4.2 ΔΕΕ υπόθεση C-362/2014, «Maximilian Schrems κατά Data Protection Commissioner»

Την απόφαση, όμως, αυτή (2000/520), με την οποία η Ευρωπαίκή Επιτροπή ενέκρινε τους κανόνες Ασφαλούς λιμένος, ακύρωσε το ΔΕΕ με απόφασή του στις 6 Οκτωβρίου 2015[33] στην υπόθεση C-362/2014, «Maximilian Schrems κατά Data Protection Commissioner» (επίτροπος προστασίας δεδομένων, στο εξής: επίτροπος) σχετικά με την άρνηση του τελευταίου να ερευνήσει καταγγελία που υπέβαλε ο M. Schrems λόγω

[32] Ιστοσελίδα του ENISA (European Union Agency for Cybersecurity), Αρχές απορρήτου Safe Harbor, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/safe-harbor-privacy-principles

[33] Βλ απόφαση ΔΕΕ της 6ης Οκτωβρίου 2015 στην υπόθεση C-362/2014, «Maximilian Schrems κατά Data Protection Commissioner», EU:C:2015:650
https://curia.europa.eu/juris/document/document.jsf;jsessionid=4D2338BD91AC1AE7CD32F9F62E983FD8?text&docid=169195&pageIndex=0&doclang=EL&mode=lst&dir&occ=first&part=1&cid=744279

του γεγονότος ότι η Facebook Ireland Ltd (στο εξής: Facebook Ireland) διαβίβασε στις Ηνωμένες Πολιτείες δεδομένα προσωπικού χαρακτήρα των χρηστών της και τα διατηρεί σε διακομιστές εγκατεστημένους στις Ηνωμένες Πολιτείες.»

Στο κείμενο της απόφασης αναφέρεται: «1. Η αίτηση προδικαστικής αποφάσεως αφορά την ερμηνεία, υπό το πρίσμα των άρθρων 7, 8 και 47 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης (στο εξής: Χάρτης), των άρθρων 25, παράγραφος 6, και 28 της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 24ης Οκτωβρίου 1995, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών (ΕΕ L 281, σ. 31)…….. καθώς επίσης, κατ' ουσίαν, και το κύρος της αποφάσεως 2000/520/ΕΚ της Επιτροπής, της 26ης Ιουλίου 2000, βάσει της οδηγίας 95/46, σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ (ΕΕ L 215, σ. 7).» και καταλήγει «…σχετικά με την επάρκεια της προστασίας που παρέχεται από τις αρχές ασφαλούς λιμένα για την προστασία της ιδιωτικής ζωής και τις συναφείς συχνές ερωτήσεις που εκδίδονται από το Υπουργείο Εμπορίου των ΗΠΑ, με την οποία η Ευρωπαϊκή Επιτροπή αποφαίνεται ότι τρίτη χώρα εξασφαλίζει ικανοποιητικό επίπεδο προστασίας, δεν εμποδίζει την αρχή ελέγχου κράτους μέλους, ……. να εξετάσει αίτηση προσώπου σχετικά με την προστασία των δικαιωμάτων και των ελευθεριών του έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που το αφορούν, τα οποία έχουν διαβιβαστεί από κράτος μέλος προς την εν λόγω τρίτη χώρα, όταν το πρόσωπο αυτό υποστηρίζει ότι η νομοθεσία και η πρακτική στην χώρα αυτή δεν εξασφαλίζουν ικανοποιητικό επίπεδο προστασίας.

2) Η απόφαση 2000/520 είναι ανίσχυρη»[34]. Συνεπώς ακυρώθηκε η απόφαση της Επιτροπής με την απόφαση του ΔΕΕ για λόγους ασυμβατότητας προς το νομικό ευρωπαϊκό πλαίσιο. Η αποκάλυψη μαζικής επεξεργασίας των δεδομένων που διαβιβάζονται στις ΗΠΑ από τις Υπηρεσίες Ασφαλείας των ΗΠΑ οδήγησε να

[34] Βλ απόφαση ΔΕΕ της 6ης Οκτωβρίου 2015 στην υπόθεση C-362/2014, «Maximilian Schrems κατά Data Protection Commissioner», EU:C:2015:650
https://curia.europa.eu/juris/document/document.jsf;jsessionid=4D2338BD91AC1AE7CD32F9F62E983FD8?text&docid=169195&pageIndex=0&doclang=EL&mode=lst&dir&occ=first&part=1&cid=744279

διαπραγματευτούν η Ευρωπαϊκή Ένωση και οι ΗΠΑ νέους αυστηρότερους κανόνες προστασίας των προσωπικών δεδομένων που διαβιβάζονται στις ΗΠΑ.

Στο μεταξύ, μια σημαντική εξέλιξη για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε χώρες εκτός ΕΟΧ, με προστασία και παροχή κατάλληλων εγγυήσεων, είχε λάβει χώρα και ήταν η θέσπιση των τυποποιημένων ρητρών της ΕΕ από την Ευρωπαϊκή Επιτροπή (2010/87/ΕΕ). Οι τυποποιημένες ρήτρες που ανέπτυξε η Ευρωπαϊκή Επιτροπή χρησιμοποιούνται σε πολλές περιπτώσεις διαβιβάσεων, όπως είναι οι διαβιβάσεις από υπευθύνους επεξεργασίας δεδομένων εγκατεστημένους στην Ε.Ε. σε εκτελούντες την επεξεργασία δεδομένων εγκατεστημένους σε τρίτες χώρες, και ιδιαίτερα χρησιμοποιούνται σε υπεργολάβους.

4.3 «Ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα» (Privacy Shield)

Την 2.2.2016 η Ευρωπαϊκή Επιτροπή συμφώνησε με τις Η.Π.Α. νέο ρυθμιστικό πλαίσιο για τη διατλαντική ροή δεδομένων με πιο προστατευτικούς κανόνες για τα διαβιβαζόμενα στις ΗΠΑ δεδομένα και δημοσίευσε την 29-2-2016 τα νομικά κείμενα που θα θέσουν σε εφαρμογή την «Ασπίδα προστασίας ΕΕ-ΗΠΑ για την ιδιωτικότητα»[35] (E.U.-U.S. Privacy Shield). Στις 12 Ιουλίου 2016 η Επιτροπή εξέδωσε απόφαση[36] στην οποία δήλωνε ότι οι ΗΠΑ εξασφαλίζουν επαρκές επίπεδο προστασίας για τα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται από την Ένωση σε οργανισμούς στις ΗΠΑ στο πλαίσιο της ασπίδας προστασίας της ιδιωτικής ζωής και το πλαίσιο αυτό άρχισε να λειτουργεί την 1η Αυγούστου 2016. Με την ασπίδα προστασίας επιτρέπεται η διαβίβαση προσωπικών δεδομένων από την ΕΕ σε μια εταιρεία στις ΗΠΑ, υπό την προϋπόθεση ότι η αμερικανική εταιρεία επεξεργάζεται

[35] Ευγενία Αλεξανδροπούλου- Αιγυπτιάδου, «ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ», εκδόσεις Νομική Βιβλιοθήκη, 2016,Βλ.διασυνοριακή ροή δεδομένων σελ.119επ.

[36] Εκτελεστική απόφαση (ΕΕ) 2016/1250 της Επιτροπής, της 12ης Ιουλίου 2016, βάσει της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ (ΕΕ L 207 της 1.8.2016, σ. 1).
https://www-enisa-europa-eu.translate.goog/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/safe-harbor-privacy-principles?_x_tr_sl=en&_x_tr_tl =el&_x_tr_hl=el&_x_tr_pto=sc

(π.χ. χρησιμοποιεί, αποθηκεύει και διαβιβάζει περαιτέρω) τα προσωπικά δεδομένα σύμφωνα με μια ισχυρή δέσμη κανόνων και διασφαλίσεων για την προστασία των δεδομένων. Για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από την ΕΕ στις ΗΠΑ διατίθενται ποικίλα εργαλεία όπως συμβατικές ρήτρες, δεσμευτικοί εταιρικοί κανόνες και η ασπίδα προστασίας της ιδιωτικής ζωής. Όταν χρησιμοποιείται η ασπίδα προστασίας της ιδιωτικής ζωής, οι εταιρείες των ΗΠΑ πρέπει να έχουν προηγουμένως εγγραφεί στο πλαίσιο αυτό μέσω του Υπουργείου Εμπορίου των ΗΠΑ.

Το Υπουργείο Εμπορίου των ΗΠΑ είναι επιφορτισμένο με την ευθύνη για τη διαχείριση και τη διοίκηση της ασπίδας προστασίας της ιδιωτικής ζωής και για να εξασφαλίζεται ότι οι εταιρείες τηρούν τις δεσμεύσεις τους. Οι εταιρείες πρέπει να εφαρμόζουν μια πολιτική προστασίας της ιδιωτικής ζωής που συνάδει με τις αρχές προστασίας της ιδιωτικής ζωής για να μπορούν να πιστοποιηθούν. Υποχρεούνται[37] δηλαδή:

- να προστατεύουν το δικαίωμα του υποκειμένου στην ενημέρωση,
-να τηρούν τους περιορισμούς σχετικά με τη χρήση των δεδομένων για διαφορετικούς σκοπούς,
-να ελαχιστοποιούν τα δεδομένα που επεξεργάζονται μόνον στον βαθμό που θεωρούνται σχετικά και απολύτως αναγκαία με τον σκοπό της επεξεργασίας και να τα διατηρούν μόνο για το διάστημα που απαιτείται, να εξασφαλίζουν ότι τα προσωπικά δεδομένα φυλάσσονται σε ασφαλές περιβάλλον και προφυλάσσονται από τυχόν απώλεια, κατάχρηση, μη εγκεκριμένη πρόσβαση, γνωστοποίηση, τροποποίηση ή καταστροφή,
-έχουν ακόμη υποχρέωση προστασίας των δεδομένων σε περίπτωση που διαβιβάζονται σε άλλη εταιρεία,
-υποχρεούνται να διασφαλίζουν την άσκηση του δικαιώματος του υποκειμένου των δεδομένων για πρόσβαση και διόρθωση των δεδομένων,
-να διασφαλίζουν την άσκηση του δικαιώματος του υποκειμένου των δεδομένων να υποβάλει καταγγελία και να λάβει έννομη προστασία,

[37] Οδηγός για την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ στην ιστοσελίδα http://ec.europa.eu, file:///C:/Users/WORKLA~1/AppData/Local/Temp/eu-us_privacy_shield_guide_el_D36C3768-C302-1CD0-601EBD84989282FC_47787-5.pdf

- να παρέχουν έννομη προστασία σε περίπτωση πρόσβασης των δημόσιων αρχών των ΗΠΑ στα προσωπικά σας δεδομένα, διασφαλίζοντας ότι αυτό θα συμβεί μόνο στον βαθμό που είναι αναγκαίο για την επίτευξη σκοπού δημόσιου συμφέροντος όπως είναι η εθνική ασφάλεια ή η επιβολή του νόμου.

Σε ετήσια βάση πρέπει να ανανεώνουν τη «συμμετοχή» τους στην ασπίδα προστασίας της ιδιωτικής ζωής. Σε περίπτωση που δεν την ανανεώσουν, δεν μπορούν πλέον δυνάμει του εν λόγω πλαισίου να λαμβάνουν και να χρησιμοποιούν δεδομένα προσωπικού χαρακτήρα από την ΕΕ.

Η Ευρωπαϊκή Επιτροπή δεσμεύτηκε να επανεξετάζει το πλαίσιο της ασπίδας προστασίας σε ετήσια βάση, ώστε να αξιολογεί αν εξακολουθεί να διασφαλίζει επαρκές επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα. Η πρώτη και η δεύτερη ετήσια επανεξέταση πραγματοποιήθηκαν τον Σεπτέμβριο του 2017 και τον Οκτώβριο του 2018, αντίστοιχα. Η έκθεση της Ευρωπαϊκής Επιτροπής για την τρίτη επανεξέταση για τη λειτουργία της ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ δημοσιεύτηκε τον Οκτώβριο του 2019[38].

Η έκθεση επιβεβαίωνε το επαρκές επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται στο πλαίσιο της ασπίδας προστασίας της ιδιωτικής ζωής από την ΕΕ σε συμμετέχουσες εταιρείες στις ΗΠΑ, κατέγραφε τη συμμετοχή περίπου 5000 εταιριών στο πλαίσιο και συνιστούσε τη λήψη συγκεκριμένων μέτρων για τη διασφάλιση της αποτελεσματικότητας της ασπίδας.

4.4 ΔΕΕ υπόθεση C-311/18 (Schrems II)

Όμως, το ΔΕΕ με την απόφαση της 16ης Ιουλίου 2020 στην υπόθεση C-311/18 (Schrems II), «Data Protection Commissioner κατά Facebook Ireland Limited και

[38] Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο «σχετικά με την τρίτη ετήσια επανεξέταση της λειτουργίας της ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ», {SWD(2019) 390 final}, Βρυξέλλες, 23.10.2019, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52019DC0495&from=ES

Maximillian Schrems»[39] καταλήγει μεταξύ άλλων και «αποφαίνεται ότι:… 4) Από την εξέταση της αποφάσεως 2010/87/ΕΕ της Επιτροπής, της 5ης Φεβρουαρίου 2010, σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε εκτελούντες επεξεργασία εγκατεστημένους σε τρίτες χώρες βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, όπως τροποποιήθηκε με την εκτελεστική απόφαση (ΕΕ) 2016/2297 της Επιτροπής, της 16ης Δεκεμβρίου 2016, υπό το πρίσμα των άρθρων 7, 8 και 47 του Χάρτη δεν προέκυψε κανένα στοιχείο ικανό να θίξει το κύρος της αποφάσεως αυτής. 5) Η εκτελεστική απόφαση (ΕΕ) 2016/1250 της Επιτροπής, της 12ης Ιουλίου 2016, βάσει της οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ, είναι ανίσχυρη». Το ΔΕΕ δήλωσε ότι το Πλαίσιο της Ασπίδας Προστασίας ΕΕ-ΗΠΑ δεν μπορούσε να παρέχει προστασία ουσιαστικά ισοδύναμη με εκείνη που εγγυάται στην ΕΕ, λόγω των νόμων επιτήρησης των ΗΠΑ που επιτρέπουν την υπερβολική συλλογή προσωπικών πληροφοριών της ΕΕ χωρίς να λαμβάνονται υπόψη οι αρχές της αναλογικότητας, της αναγκαιότητας και της επανόρθωσης[40].

Συνεπώς στις 16 Ιουλίου 2020, το Ευρωπαϊκό Δικαστήριο ακύρωσε την ασπίδα προστασίας (Privacy Shield) ΕΕ-ΗΠΑ επιβεβαιώνοντας παράλληλα την εγκυρότητα των Τυποποιημένων Συμβατικών Ρήτρων ("SCC") της ΕΕ για τη μεταφορά προσωπικών δεδομένων σε εκτελούντες την επεξεργασία εκτός ΕΕ/ΕΟΧ, «υπό συγκεκριμένες προϋποθέσεις. Ειδικότερα, πριν από οποιαδήποτε διαβίβαση με βάση τις SCC, ο εξαγωγέας −με τη βοήθεια του εισαγωγέα των δεδομένων− πρέπει να εξετάζει εάν το επίπεδο προστασίας των δεδομένων το οποίο κατοχυρώνει ο ΓΚΠΔ, εξασφαλίζεται στην εκάστοτε τρίτη χώρα, λαμβάνοντας υπόψη τις συνθήκες της συγκεκριμένης διαβίβασης και πρόσθετα μέτρα που μπορεί αυτός να λάβει. Σε περίπτωση δε που καταλήξει στο συμπέρασμα ότι δεν παρέχεται επαρκές επίπεδο

[39] Βλ. απόφαση ΔΕΕ της 16ης Ιουλίου 2020 στην υπόθεση C-311/18 (Schrems II), «Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems», EU:C:2020:559, https://curia.europa.eu/juris/liste.jsf?num=C-311/18
https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62018CJ0311

[40] Mallory Petroli, Stubbs Alderton & Markiles, LLP, National Law Review, Τόμος XI, Αριθμός 221,"New Standard Contractual Clauses Under the GDPR", August 9, 2021, page 2.

προστασίας, ο εξαγωγέας πρέπει να αναστείλει τη διαβίβαση ή/και να καταγγείλει τη σύμβαση με τον εισαγωγέα»[41].

4.5 Πρότυπο ISO/IEC 27018

Στην κατεύθυνση της διασφάλισης της συμμόρφωσης από πλευράς των παρόχων υπηρεσιών cloud computing αξίζει να επισημανθεί η υιοθέτηση των προδιαγραφών ISO/IEC 27018 : 2014 [42] . Το ISO/IEC 27018 :2014 είναι το πρώτο ισχυρό και διεθνώς αναγνωρισμένο σημείο αναφοράς για την προστασία των προσωπικών πληροφοριών (personal identifiable information-PII) που είναι αποθηκευμένες στο cloud[43].

Χρησιμοποιώντας ως θεμέλιό του το προϋφιστάμενο ISO/IEC 27001:2013, ένα παγκοσμίως καθιερωμένο δηλαδή πρότυπο συστημάτων διαχείρισης ασφάλειας πληροφοριών (ISMS), που παρείχε ένα ευέλικτο σύστημα για τον εντοπισμό κινδύνων ασφάλειας των πληροφοριών και την επιλογή των ελέγχων για την αντιμετώπισή τους, το ISO/IEC 27018:2014 προσφέρει πλέον συγκεκριμένες οδηγίες – προδιαγραφές για να βοηθήσει τους Παρόχους Υπηρεσιών Cloud (CSP) να αξιολογήσουν τους κινδύνους, και να εφαρμόσουν κατάλληλους ελέγχους τελευταίας τεχνολογίας για την προστασία των Προσωπικών Αναγνωριστικών Πληροφοριών (PII) που είναι αποθηκευμένες στο cloud[44]. Ήτοι, το ISO/IEC 27018:2014 «θεσπίζει κοινά αποδεκτούς στόχους ελέγχου, ελέγχους και κατευθυντήριες γραμμές για την εφαρμογή μέτρων για την προστασία των PII σύμφωνα με τις αρχές απορρήτου του ISO/IEC 29100 για το δημόσιο περιβάλλον υπολογιστικού νέφους. Το ISO/IEC 27018:2014 ισχύει για όλους τους τύπους και τα μεγέθη οργανισμών, συμπεριλαμβανομένων δημόσιων και ιδιωτικών εταιρειών, κρατικών οντοτήτων και μη κερδοσκοπικών

[41] https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/schrems_II

[42] Βλ. αναλυτικότερα ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), ISO/IEC 27018:2014, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (Τεχνολογία της πληροφορίας — Τεχνικές ασφαλείας — Κώδικας πρακτικής για την προστασία προσωπικών πληροφοριών (PII) σε δημόσια σύννεφα που λειτουργούν ως εκτελούντες την επεξεργασία PII)

[43] https://www-iso-org.translate.goog/news/2015/07/Ref1983.html?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc

[44] Λίλιαν Μήτρου, Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, Νομική Βιλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 4/2015, Οκτώβριος - Νοέμβριος – Δεκέμβριος 2015, σελ.549

οργανισμών, που παρέχουν υπηρεσίες επεξεργασίας πληροφοριών ως επεξεργαστές PII μέσω υπολογιστικού νέφους βάσει σύμβασης με άλλους οργανισμούς[45].

Η εταιρία Microsoft ήταν ο πρώτος μεγάλος CSP που υιοθέτησε τις αυστηρές αρχές απορρήτου που περιγράφονται στο πρότυπο ISO/IEC 27018 και υποβάλει τις υπηρεσίες cloud της σε ανεξάρτητο έλεγχο αυτών των ελέγχων. Αξίζει να σημειωθεί ότι το ISO/IEC 27018:2014 αναθεωρήθηκε σχετικά πρόσφατα και δημοσιεύτηκε το ISO/IEC 27018:2019.

4.6 Από την απόφαση επάρκειας στην παροχή κατάλληλων εγγυήσεων

Βάσει του δικαίου της ΕΕ[46], «η διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτη χώρα ή διεθνή οργανισμό μπορεί να πραγματοποιηθεί εφόσον η Επιτροπή έχει αποφασίσει ότι διασφαλίζεται επαρκές επίπεδο προστασίας από την τρίτη χώρα, από έδαφος ή από έναν ή περισσότερους συγκεκριμένους τομείς στην εν λόγω τρίτη χώρα ή από τον εν λόγω διεθνή οργανισμό. Για μια τέτοια διαβίβαση δεν απαιτείται ειδική άδεια». Επιτρέπεται δηλαδή η αντίστοιχη διαβίβαση βάσει απόφασης επάρκειας την οποία εκδίδει η Επιτροπή με εξειδικευμένα κριτήρια και προϋποθέσεις[47].

Όταν δεν υπάρχει η ανωτέρω απόφαση επάρκειας, οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό επιτρέπονται, χωρίς να απαιτείται ειδική άδεια της εποπτικής αρχής, εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία παρέχει κατάλληλες εγγυήσεις και εάν υφίστανται εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα για τα υποκείμενα των δεδομένων[48]. Ο κατάλογος των «κατάλληλων εγγυήσεων» που είναι αποδεκτές προβλέπεται αποκλειστικά στο δίκαιο της ΕΕ για την προστασία δεδομένων[49].

[45] https://www-iso-org.translate.goog/standard/61498.html?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc
[46] Άρθρο 45 παρ. 1 ΓΚΠΔ
[47] Άρθρο 45 παρ. 2 επ. ΓΚΠΔ
[48] άρθρο 46 παρ. 1 ΓΚΠΔ.
[49] άρθρο 46 παρ. 2 ΓΚΠΔ.

Κατάλληλες εγγυήσεις μπορούν να προβλέπονται μέσω[50]:

• ενός νομικά δεσμευτικού και εκτελεστού μέσου για δημόσιες αρχές ή φορείς,
• δεσμευτικών εταιρικών κανόνων,
• τυποποιημένων ρητρών προστασίας δεδομένων που εκδίδονται είτε από την Ευρωπαϊκή Επιτροπή είτε από εποπτική αρχή και εγκρίνονται από την Επιτροπή,
• κωδίκων δεοντολογίας,
• μηχανισμών πιστοποίησης .

4.7 Δεσμευτικοί Εταιρικοί Κανόνες (BCR)

Βάσει του εφαρμοστέου ΓΚΠΔ περιλαμβάνονται στις κατάλληλες εγγυήσεις που επιτρέπουν διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, χωρίς να απαιτείται ειδική άδεια της εποπτικής αρχής, και οι εταιρικοί δεσμευτικοί κανόνες[51].

Σύμφωνα με το άρθρο 4 παρ. 20 του ΓΚΠΔ, δεσμευτικοί εταιρικοί κανόνες (BCR) είναι οι πολιτικές προστασίας προσωπικών δεδομένων τις οποίες ακολουθεί ένας υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία εγκατεστημένος στο έδαφος κράτους μέλους για διαβιβάσεις δεδομένων σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία σε μία ή περισσότερες τρίτες χώρες εντός ομίλου επιχειρήσεων ή ομίλου εταιρειών που ασκεί κοινή οικονομική δραστηριότητα[52].

Λόγω της εφαρμογής του ΓΚΠΔ και των αλλαγών που αυτός έφερε, πρέπει όλοι οι όμιλοι επιχειρήσεων που διαβιβάζουν προσωπικά δεδομένα με βάση BCR ήδη εγκεκριμένα κατά την Οδηγία 95/46 να τα τροποποιήσουν ώστε να είναι συμβατά με τον ΓΚΠΔ. Για τον λόγο αυτό, οι ανωτέρω όμιλοι επιχειρήσεων καλούνται να

[50] «Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων, Έκδοση 2018», Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, 2019, σελ.325-326,
https://www.echr.coe.int/Documents/Handbook_data_protection_ELL.pdf
[51] «Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων ,Έκδοση 2018», Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, 2019, σελ.330,
https://www.echr.coe.int/Documents/Handbook_data_protection_ELL.pdf
[52] Βλ. Εισ. Σκ. 110 ΓΚΠΔ

κοινοποιήσουν, κατ' εκπλήρωση της σχετικής υποχρέωσής του[53] τις σχετικές τροποποιήσεις των δεσμευτικών εταιρικών κανόνων τους σε όλα τα μέλη του ομίλου και στις εποπτικές αρχές, μέσω της επικεφαλής εποπτικής αρχής, στο πλαίσιο της ετήσιας ενημέρωσής τους, αρχής γενομένης από την 25η Μαΐου 2018 έναρξη ισχύος του ΓΚΠΔ. Οι επικαιροποιημένοι δεσμευτικοί εταιρικοί κανόνες μπορούν να χρησιμοποιηθούν χωρίς να είναι αναγκαία η υποβολή αίτησης για τη χορήγηση νέας άδειας ή έγκρισης.

Η αρμόδια Εποπτική Αρχή εγκρίνει τα BCR σύμφωνα με τον μηχανισμό συνεκτικότητας του άρθρου 63 ΓΚΠΔ. Ανακοινώνει το σχέδιο απόφασής της στο ΕΣΠΔ, το οποίο με τη σειρά του εκδίδει γνώμη σχετικά με τα BCR. Εάν το ΕΣΠΔ εκδώσει σύμφωνη γνώμη για τα υπό εξέταση BCR, η αρμόδια Εποπτική Αρχή προχωρά στην έγκρισή τους, λαμβάνοντας «ιδιαιτέρως» υπόψη τη γνώμη του Συμβουλίου Προστασίας Δεδομένων. Η γνώμη αυτή δεν είναι νομικά δεσμευτική, αλλά εάν η εποπτική αρχή προτίθεται να μην τη λάβει υπόψη, τότε ενεργοποιείται ο μηχανισμός επίλυσης διαφορών και το Συμβούλιο Προστασίας Δεδομένων θα κληθεί να εκδώσει νομικά δεσμευτική απόφαση, με πλειοψηφία δύο τρίτων των μελών του[54].

Στους δεσμευτικούς εταιρικούς κανόνες πρέπει να προσδιορίζονται, μεταξύ άλλων, τα δικαιώματα των υποκειμένων των δεδομένων και να υπάρχει πρόβλεψη ρύθμισης για ευθύνη από τυχόν παράβαση των κανόνων[55].

4.8 Τυποποιημένες συμβατικές ρήτρες για τις διεθνείς διαβιβάσεις δεδομένων

Η Ευρωπαϊκή Επιτροπή έχει θέσει σε ισχύ από τις 27-6-2021 νέες πρότυπες τυποποιημένες συμβατικές ρήτρες για τις διαβιβάσεις δεδομένων προς τρίτες χώρες δυνάμει της Εκτελεστικής Απόφασης (ΕΕ) 2021/914 της Επιτροπής της 4ης Ιουνίου

[53] βλ. σημείο 5.1 του εγγράφου εργασίας WP153, « Έγγραφο εργασίας για την κατάρτιση πίνακα με τα στοιχεία και τις αρχές που πρέπει να περιέχονται στους δεσμευτικούς εταιρικούς κανόνες» , εκδόθηκε στις 28 Νοεμβρίου 2017 και τελικά αναθεωρήθηκε και εκδόθηκε στις 6 Φεβρουαρίου 2018.

[54] Βάσει άρθρου 57 παράγραφος 1 στοιχείο ιθ), άρθρο 58 παράγραφος 3 στοιχείο ι), άρθρο 64 παράγραφος 1 στοιχείο στ), άρθρο 65 παράγραφοι 1 και 2 ΓΚΠΔ.

[55] Γενικός Κανονισμός για την Προστασία Δεδομένων, άρθρο 47, παρ.2 εδ. ε΄,στ΄.

2021 σχετικά με τις τυποποιημένες συμβατικές ρήτρες για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα προς τρίτες χώρες -εκτός ΕΕ-ΕΟΧ- σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Οι νέες τυποποιημένες συμβατικές ρήτρες (εφεξής SCC) συνάδουν με τις απαιτήσεις του ΓΚΠΔ καθώς και τα συμπεράσματα στα οποία κατέληξε το ΔΕΕ στην απόφαση Schrems II, και έχουν ως στόχο να πετύχουν ένα υψηλό επίπεδο προστασίας των προσωπικών δεδομένων, λαμβάνοντας υπόψη τις προκλήσεις που αντιμετωπίζουν οι επιχειρήσεις στη σύγχρονη ψηφιακή εποχή[56].

Οι καινοτομίες των SCC εντοπίζονται κυρίως:
«-στην εναρμόνιση με τις ρυθμίσεις του ΓΚΠΔ
-στην παροχή πρακτικών οδηγιών συμμόρφωσης με την απόφαση Schrems II και
-στην παροχή περισσότερης ευελιξίας μέσω του συνδυασμού γενικών ρητρών με μια προσέγγιση βάσει ενοτήτων (modular approach), ώστε να λαμβάνονται υπόψη διάφορα σενάρια διαβίβασης, καθώς και η πολυπλοκότητα των σύγχρονων αλυσίδων επεξεργασίας, που συχνά περιλαμβάνουν τη συμμετοχή περισσοτέρων από δύο μερών στη διαβίβαση»[57].

Συγκεκριμένα, οι SCC περιλαμβάνουν τέσσερις ενότητες για τη ρύθμιση των διαβιβάσεων[58]:

- η πρώτη ενότητα ρυθμίζει διαβιβάσεις από υπεύθυνο επεξεργασίας σε υπεύθυνο επεξεργασίας,
- η δεύτερη ενότητα ρυθμίζει διαβιβάσεις από υπεύθυνο επεξεργασίας σε εκτελούντα την επεξεργασία,
- η τρίτη ενότητα ρυθμίζει διαβιβάσεις από εκτελούντα την επεξεργασία σε εκτελούντα την επεξεργασία,
- η τέταρτη ενότητα ρυθμίζει διαβιβάσεις από εκτελούντα την επεξεργασία σε υπεύθυνο επεξεργασίας.

[56] ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ, https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/simvatikes_ritres
[57] Βλ. ανωτέρω υποσημείωση υπ΄αρ.56
[58] Βλ. Εκτελεστική Απόφαση (ΕΕ) 2021/914 της Επιτροπής, Τμήμα ΙΙΙ των ρητρών, «Τοπική νομοθεσία και υποχρεώσεις σε περίπτωση πρόσβασης από τις δημόσιες αρχές», Ρήτρα 14 και 15, σελ. 22,23)

Με τις νέες SCC προβλέπεται μεταβατική περίοδος 18 μηνών, ήτοι από την έναρξη ισχύος τους στις 27-6-21 ως τις 27-12-2022, για την αντικατάσταση των προηγούμενων (2001/497/ΕΚ και 2010/87/ΕΕ που εγκρίθηκαν βάσει της προηγούμενης Οδηγίας 95/46 για την Προστασία Δεδομένων) με τις καινούριες. Επίσης, οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία μπορούν να συνεχίσουν να χρησιμοποιούν τις προηγούμενες SCC (2001/497/ΕΚ και 2010/87/ΕΕ), για τρεις μήνες από την έναρξη ισχύος των νέων ρητρών(27-6-2021), ήτοι έως τις 27-9-21 [59]. Επομένως, από τις 27 Σεπτεμβρίου 2021 δεν είναι πλέον δυνατή η σύναψη συμβάσεων με ενσωματώση των ανωτέρω αναφερόμενων προηγούμενων SCC. Ενώ οι προηγούμενες SCC μπορούν να συνεχίσουν να χρησιμοποιούνται ως τις 27-12-2022 μόνο για τις συμβάσεις που είχαν συναφθεί πριν από τις 27 Σεπτεμβρίου 2021, υπό την προϋπόθεση ότι οι εργασίες επεξεργασίας που αποτελούν το αντικείμενο της σύμβασης παραμένουν αμετάβλητες και ότι η επίκληση των προηγούμενων από αυτές ρητρών διασφαλίζει ότι η διαβίβαση δεδομένων προσωπικού χαρακτήρα υπόκειται σε κατάλληλες εγγυήσεις.

Οι SCC είναι σύνολα τυποποιημένων συμβατικών όρων και προϋποθέσεων που αποδέχονται και υπογράφουν τόσο ο αποστολέας όσο και ο παραλήπτης των προσωπικών δεδομένων και προορίζονται να παρέχουν διασφάλιση κατάλληλων εγγυήσεων, σύμφωνα με το άρθρο 46 του ΓΚΠΔ, μέσω συμβατικών υποχρεώσεων ως προς το ότι η προστασία των δεδομένων βρίσκεται στο επίπεδο που απαιτείται σύμφωνα με τον ΓΚΠΔ στις διεθνείς διαβιβάσεις. Με τις SCC καθορίζονται τα δικαιώματα και οι υποχρεώσεις τόσο του υπευθύνου επεξεργασίας δεδομένων όσο και του εκτελούντος την επεξεργασία δεδομένων, όταν επεξεργάζονται προσωπικά δεδομένα για λογαριασμό του υπευθύνου επεξεργασίας δεδομένων. Είναι εύχρηστοι όροι που θα μπορούσαν να άρουν την ανάγκη για διαπραγμάτευση μεμονωμένων συμβάσεων. Μπορούν να προστεθούν βέβαια σε υπάρχουσες συμβάσεις.

«Ως εκ τούτου, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία που διαβιβάζει τα δεδομένα προσωπικού χαρακτήρα σε τρίτη χώρα (στο εξής: εξαγωγέας των δεδομένων) και ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία που λαμβάνει

[59] Άρθρο 4 της Εκτελεστικής Απόφασης (ΕΕ) 2021/914 της Επιτροπής, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32021D0914&from=EN

τα δεδομένα προσωπικού χαρακτήρα (στο εξής: εισαγωγέας των δεδομένων) είναι ελεύθεροι να ενσωματώνουν τις εν λόγω τυποποιημένες συμβατικές ρήτρες σε ευρύτερη σύμβαση και να προσθέτουν άλλες ρήτρες ή πρόσθετες εγγυήσεις εφόσον αυτές δεν αντιφάσκουν, άμεσα ή έμμεσα, προς τις τυποποιημένες συμβατικές ρήτρες ούτε θίγουν τα θεμελιώδη δικαιώματα ή τις ελευθερίες των υποκειμένων των δεδομένων. Οι υπεύθυνοι επεξεργασίας και οι εκτελούντες την επεξεργασία ενθαρρύνονται[60] να παράσχουν πρόσθετες εγγυήσεις μέσω συμβατικών δεσμεύσεων που δρουν συμπληρωματικά ως προς τις τυποποιημένες συμβατικές ρήτρες» [61].

Τα SCC είναι μία από τις διασφαλίσεις που μπορούν να χρησιμοποιηθούν για τη συμμόρφωση με τον ΓΚΠΔ και είναι αυτή που είναι πιο πιθανό να χρησιμοποιηθεί από τις μικρές και μεσαίες επιχειρήσεις. Με τον τρόπο αυτό στοχεύουν και συμβάλλουν στην ενοποίηση της προσέγγισης για τη διασυνοριακή επεξεργασία και συνεισφέρουν στη διασφάλιση της ελεύθερης ροής προσωπικών δεδομένων.

4.9 Κώδικες δεοντολογίας (CoC)

Οι κώδικες δεοντολογίας έχουν ως στόχο να διευκολύνουν την εφαρμογή και την εναρμόνιση με τους κανόνες του ΓΚΠΔ ρυθμίζοντας ειδικές υποχρεώσεις τόσο για τους υπεύθυνους επεξεργασίας όσο και για τους εκτελούντες την επεξεργασία, για ειδικούς τομείς δραστηριότητας[62]. Οι κώδικες αυτοί εκπονούνται από ενώσεις ή άλλους φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία, λαμβάνοντας υπόψη τα ειδικά χαρακτηριστικά των διαφόρων τομέων επεξεργασίας. Όταν το σχέδιο κώδικα δεοντολογίας αφορά επεξεργασία προσωπικών δεδομένων σε διάφορα κράτη μέλη, τότε η ένωση ή ο φορέας που τον καταρτίζει τον υποβάλλει σε μια αρμόδια εποπτική αρχή (τεκμηριώνοντας για ποιο λόγο κρίθηκε η εν λόγω εποπτική αρχή ως αρμόδια. Θα μπορούσαν να ληφθούν υπόψη ορισμένοι παράγοντες, όπως η τοποθεσία της μεγαλύτερης σε πυκνότητα δραστηριότητας της επεξεργασίας ή την τοποθεσία της έδρας του κατόχου του κώδικα[63]). Στη συνέχεια η

[60] Εκτελεστική Απόφαση (ΕΕ) 2021/914 της Επιτροπής, σελ.1, σημείωση 3.
[61] Αιτιολογική σκέψη 109 του Κανονισμού (ΕΕ) 2016/679 (ΓΚΠΔ)
[62] Άρθρο 40 παρ.1 ΓΚΠΔ
[63] Γνώμη 16/2021της 19ης Μαΐου 2021 του ΕΣΠΔ, σελ. 5, παρ. 7.

αρμόδια εποπτική αρχή υποβάλλει το σχέδιο στο Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (ΕΣΠΔ) (σύμφωνα με το μηχανισμό συνεκτικότητας), το οποίο γνωμοδοτεί ως προς τη συμμόρφωση του σχεδίου προς τον ΓΚΠΔ. Αν η γνωμοδότηση του ΕΣΠΔ είναι θετική, διαβιβάζεται στην Επιτροπή, η οποία προχωράει στην έγκρισή του και μπορεί, μέσω εκτελεστικών πράξεων, να αποφασίζει ότι οι εγκεκριμένοι κώδικες δεοντολογίας (και οι τυχόν τροποποιήσεις ή επεκτάσεις τους) έχουν γενική ισχύ εντός της Ένωσης[64].

4.9.1 EU Cloud Code of Conduct - CoC

Ένας πρόσφατος και σύγχρονος κώδικας είναι ο Κώδικας Δεοντολογίας Νέφους της ΕΕ (EU Cloud Code of Conduct - CoC), που σχεδιάστηκε για να συμβάλει στη δημιουργία ενός περιβάλλοντος εμπιστοσύνης και διαφάνειας στην ευρωπαϊκή αγορά υπολογιστικής νέφους και να απλοποιήσει τη διαδικασία αξιολόγησης κινδύνου όσον αφορά την παροχή υπηρεσιών cloud από παρόχους υπηρεσιών cloud (CSP) σε πελάτες cloud (CSC). Όπως χαρακτηριστικά αναφέρεται στην επίσημη ιστοσελίδα του Κώδικα αυτού : «Είναι ο πρώτος Διακρατικός Κώδικας Δεοντολογίας που καλύπτει όλες τις προσφορές cloud, που εγκρίνεται. Θα διευκολύνει τους χρήστες υπηρεσιών cloud – ιδιαίτερα τις ΜΜΕ και τους δημόσιους φορείς– να προσδιορίσουν εάν μια δεδομένη υπηρεσία που βασίζεται σε υπολογιστικό νέφος είναι συμβατή με το GDPR.

Με αυτόν τον τρόπο, θα οικοδομήσει εμπιστοσύνη στις διαδικτυακές υπηρεσίες και θα αυξήσει το προεπιλεγμένο επίπεδο προστασίας δεδομένων στην ευρωπαϊκή αγορά υπολογιστικού νέφους, συμβάλλοντας τελικά στην επιτάχυνση της υιοθέτησης αυτής της βασικής τεχνολογίας και θα φέρει τα οφέλη του υπολογιστικού νέφους σε ένα ευρύτερο τμήμα της ευρωπαϊκής οικονομίας»[65].

Ο EU Cloud Code of Conduct(CoC) εγκρίθηκε από τη Βελγική Εποπτική Αρχή στις 20 Μαΐου 2021, βάσει θετικής γνώμης του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων[66]. Το ΕΣΠΔ στη θετική Γνώμη που εξέδωσε ενόψει της έγκρισης του

[64] https://www.dpa.gr/el/foreis/kwdikes_deodologias
[65] https://eucoc.cloud/en/detail/news/the-eu-cloud-code-of-conduct-becomes-first-gdpr-code-of-conduct-to-receive-green-light-from-data-pro/
[66] Γνώμη 16/2021 της 19ης Μαΐου 2021 του ΕΣΠΔ,

Κώδικα, υπογραμμίζει ότι οι κώδικες δεοντολογίας είναι εργαλεία εθελοντικής λογοδοσίας και ότι η τήρηση ενός τέτοιου κώδικα δεν εμποδίζει τις Εποπτικές Αρχές (ΕΑ) να ασκήσουν τον έλεγχο, την εξουσία επιβολής και τα προνόμιά που αυτές έχουν. Ακόμη σημειώνει ότι ο Κώδικας Δεοντολογίας Cloud της ΕΕ προορίζεται για την αντιμετώπιση όλων των τεχνικών εκδοχών παροχής υπηρεσιών cloud (π.χ. IaaS, PaaS, SaaS) και δημιουργεί μια «βασική γραμμή για την εφαρμογή του GDPR» για αυτές τις υπηρεσίες. Κρίνει ακόμη ότι σκοπός του Κώδικα είναι να παρέχει πρακτική καθοδήγηση και να ορίζει συγκεκριμένες απαιτήσεις για τους παρόχους υπηρεσιών cloud ("CSP"). Και μάλιστα διευκρινίζει ότι ισχύει μόνο για υπηρεσίες cloud όπου ο CSP ενεργεί ως εκτελών την επεξεργασία. Εξ αντιδιαστολής προκύπτει ότι δεν ισχύει για υπηρεσίες «επιχειρείν προς καταναλωτή» (B2C) ή για οποιεσδήποτε δραστηριότητες επεξεργασίας για τις οποίες ο CSP μπορεί να λειτουργεί ως υπεύθυνος επεξεργασίας δεδομένων. Ο Κώδικας, όμως, από μόνος του αφορά επίσης τους καταναλωτές που θα λάβουν πρόσθετες εγγυήσεις συμμόρφωσης όταν εμπιστεύονται τα προσωπικά τους δεδομένα σε μια εταιρεία που χρησιμοποιεί έναν εκτελούντα την επεξεργασία που εφαρμόζει τον Κώδικα[67]. Ο EU Cloud Code of Conduct αναπτύχθηκε από την SCOPE Europe, μια ανεξάρτητη ένωση τρίτων μερών, σε συνεργασία με αρκετούς παράγοντες του κλάδου.

Η SCOPE Europe σύμφωνα με την επίσημη ιστοσελίδα της [68]«ιδρύθηκε τον Φεβρουάριο του 2017 ως θυγατρική του γερμανικού μη κερδοσκοπικού οργανισμού SRIW e.V. (Selbstregulierung Informationswirtschaft – Αυτορύθμιση της Οικονομίας της Πληροφορίας) και, τον Μάιο του 2021, έγινε ο πρώτος Φορέας Παρακολούθησης που διαπιστεύτηκε βάσει του Ευρωπαϊκού Γενικού Κανονισμού για την Προστασία Δεδομένων σύμφωνα με το άρθρο 41. Η SCOPE Europe είναι μια ένωση που υποστηρίζει τη συνρύθμιση της οικονομίας της πληροφορίας. Λειτουργεί ως δεξαμενή σκέψης για τη συζήτηση βασικών θεμάτων στην ψηφιακή πολιτική και παρέχει έναν οργανισμό-ομπρέλα για μια σειρά από συν-ρυθμιστικά μέτρα στον ψηφιακό κλάδο.

https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgiansupervisory_el

[67] Γνώμη 16/2021της 19ης Μαΐου 2021 του ΕΣΠΔ, σελ. 5

[68] https://scope-europe.eu/en/our-scope/about-us.html

Ο David Stevens, Πρόεδρος της Βελγικής Αρχής Προστασίας Δεδομένων, της αρμόδιας αρχής προστασίας δεδομένων για τον Κώδικα Δεοντολογίας, δήλωσε: «η έγκριση του EU Cloud CoC επιτεύχθηκε μέσω στενής συνεργασίας με το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων και είναι ένα σημαντικό βήμα προς μια εναρμονισμένη ερμηνεία και εφαρμογή του ΓΚΠΔ σε έναν κρίσιμο τομέα για την ψηφιακή οικονομία.

Ελπίζω ότι αυτή η πρώτη εμπειρία στην έγκριση ενός διακρατικού κώδικα δεοντολογίας θα σηματοδοτήσει την αρχή της ανάπτυξης περισσότερων διακρατικών κωδίκων δεοντολογίας για την προώθηση της συμμόρφωσης για τις εταιρείες, την εναρμόνιση για τους τομεακούς οργανισμούς και τη διαφάνεια για τα υποκείμενα των δεδομένων»[69].

4.9.2 Code of conduct of CISPE

Ένας ακόμη πολύ πρόσφατος αλλά πιο εξειδικευμένος κώδικας δεοντολογίας είναι ο ευρωπαϊκός κώδικας δεοντολογίας των Παρόχων Υπηρεσιών Υποδομής Cloud. Πρόκειται για έναν πρακτικό οδηγό σχετικά με την εφαρμογή του ΓΚΠΔ και τη συμμόρφωση με αυτόν συγκεκριμένα από τους παρόχους υπηρεσιών IaaS (CISP) , που περιλαμβάνει τα πραγματικά μέτρα που πρέπει αυτοί να λάβουν. Το σχέδιο του κώδικα Δεοντολογίας CISPE αναπτύχθηκε από τον CISPE, τον Ευρωπαϊκό Οργανισμό Παρόχων Υποδομής Νέφους, μια μη κερδοσκοπική ένωση με έδρα το Βέλγιο. Υποβλήθηκε στη συνέχεια στη Γαλλική Εποπτική Αρχή (FR SA), η οποία κρίθηκε αρμόδια σύμφωνα με κάποια κριτήρια, όπως η εγκατάσταση πολλών μελών και στελεχών του CISPE συμπεριλαμβανομένων του ταμία και των εταιρειών του προέδρου στη Γαλλία[70]. Με τη σειρά της η FR SA υπέβαλε το σχέδιο απόφασής για το σχέδιο του Κώδικα Δεοντολογίας CISPE στο ΕΣΠΔ, σύμφωνα με το άρθρο 64 παρ. 1 στοιχείο β΄ ΓΚΠΔ στις 29 Φεβρουαρίου 2021, ζητώντας τη γνώμη του, ενώ το αρχείο της σχετικής απόφασης της για πληρότητα του σχεδίου κώδικα δόθηκε στις 31 Μαρτίου 2021. Το ΕΣΠΔ εξέδωσε τη θετική γνώμη του στις 19 Μαϊου 2021 [71]. Τέλος,

[69] Από την επίσημη ιστοσελίδα του EU Cloud Code of Conduct, https://eucoc.cloud/en/detail/news/the-eu-cloud-code-of-conduct-becomes-first-gdpr-code-of-conduct-to-receive-green-light-from-data-pro/

[70] Γνώμη 17/2021της 19ης Μαϊου 2021 του EDPB, σελ. 5 , παρ. 9.

[71] Γνώμη 17/2021της 19ης Μαϊου 2021 του EDPB

η Γαλλική Εποπτική Αρχή (άλλως η Γαλλική Αρχή Προστασίας Δεδομένων- CNIL) τον Ιούνιο του 2021 αποδέχτηκε και ενέκρινε τον Κώδικα Δεοντολογίας CISPE, ο οποίος είναι ο πρώτος ευρωπαϊκός κώδικας δεοντολογίας αφιερωμένος στους παρόχους μιας συγκεκριμένης μόνο τεχνικής εκδοχής του υπολογιστικού νέφους, του IaaS. Αντιμετωπίζει τους συγκεκριμένους ρόλους και τις ευθύνες των παρόχων IaaS.

Σύμφωνα με την επίσημη ιστοσελίδα του CISPE[72] ο Κώδικας:

- Δίνει ένα πλαίσιο συμμόρφωσης με τον GDPR.
- Αποκλείει την επαναχρησιμοποίηση των δεδομένων των πελατών IaaS, καθώς οι πάροχοι δηλωμένων υπηρεσιών «θα έχουν πρόσβαση ή θα χρησιμοποιούν δεδομένα πελατών μόνο για τη διατήρηση ή την παροχή της υπηρεσίας και δεν θα χρησιμοποιούν δεδομένα πελατών για σκοπούς μάρκετινγκ ή διαφήμισης».
- Επιτρέπει τους πελάτες να επιλέξουν να επεξεργάζονται και να αποθηκεύουν τα δεδομένα τους αποκλειστικά εντός του Ε.Ο.Χ.
- Προσδιορίζει ποιες Υπηρεσίες Υποδομής Cloud είναι κατάλληλες για την επεξεργασία δεδομένων που θέλουν να εκτελέσουν.
- Βοηθά τους πολίτες να ανακτήσουν τον έλεγχο των δεδομένων τους.

Ένα ακόμη σημαντικό στοιχείο του Κώδικα είναι ότι η συμμόρφωση με αυτόν επαληθεύεται από ανεξάρτητους, εξωτερικούς ελεγκτές, διαπιστευμένους ως «Φορείς Παρακολούθησης» από την αρμόδια Ευρωπαϊκή Αρχή Προστασίας Δεδομένων. Οι ανεξάρτητοι «Φορείς Παρακολούθησης» ενισχύουν το επίπεδο διασφάλισης που παρέχεται από υπηρεσίες που δηλώνονται βάσει του κώδικα[73].

Ο Κώδικας χωρίζεται σε πέντε μέρη. «Κάθε μέρος παρέχει πρακτικές εξηγήσεις για τα ζητήματα που αντιμετωπίζει ο κλάδος και παρέχει συγκεκριμένα παραδείγματα για να βοηθήσει τα μέλη του κώδικα να κατανοήσουν τις υποχρεώσεις τους για την προστασία δεδομένων»[74].

[72] https://cispe.cloud/code-of-conduct
[73] https://www.codeofconduct.cloud
[74] https://www.cnil.fr/en/cnil-approves-first-european-code-conduct-cloud-infrastructure-service-providers-iaas

5 Συμβάσεις υπολογιστικού νέφους

5.1 Περιεχόμενο των συμβάσεων υπολογιστικού νέφους

Οι συμβάσεις υπολογιστικού νέφους είναι οι συμβάσεις που συνάπτονται ανάμεσα στον πάροχο των υπηρεσιών και στους χρήστες-πελάτες με κεντρικό άξονα τις παρεχόμενες υπηρεσίες στο «σύννεφο». Οι συμβάσεις αυτές καλούνται να ρυθμίσουν μια σειρά θεμάτων, ενδεικτικά να προσδιορίσουν τα δικαιώματα και τις υποχρεώσεις των μερών, τον ρόλο του καθενός ως προς την επεξεργασία προσωπικών δεδομένων, την ευθύνη από τυχόν παραβίαση των όρων της σύμβασης, το εφαρμοστέο δίκαιο αλλά και τη δικαιοδοσία για επίλυση τυχόν εκ συμβάσεως διαφορών, να προσδιορίσουν επαρκώς τα τηρούμενα μέτρα ασφαλείας, να περιλάβουν ρήτρες εμπιστευτικότητας, να παρέχουν εγγυήσεις για την προστασία των προσωπικών δεδομένων και την τήρηση του απορρήτου, όρους για τη λήξη ή τη λύση/ καταγγελία της σύμβασης, και γενικά όλα τα απαραίτητα σε μια σύμβαση στοιχεία, αλλά μέσα στο πλαίσιο της πολυεπίπεδης δομής του υπολογιστικού νέφους, στο οποίο ο χρήστης έχει πρόσβαση σε απείρως επεκτάσιμες και ευέλικτες δυνατότητες ΤΠ ανάλογα με τις ανάγκες του.

Ωστόσο, η τεράστια ευελιξία της αρχιτεκτονικής και του σχεδιασμού της τεχνολογίας του υπολογιστικού νέφους, συχνά αντισταθμίζεται από μειωμένη βεβαιότητα για τον πελάτη, εξαιτίας ελλιπώς διατυπωμένων και μη συγκεκριμενοποιημένων συμβάσεων με τους παρόχους υπολογιστικού νέφους. Οι περισσότεροι πάροχοι προσφέρουν «ετοιμοπαράδοτες» υπηρεσίες σε πολλαπλούς χρήστες με αποτέλεσμα οι καταρτιζόμενες συμβάσεις να ’ναι κατά κανόνα τυποποιημένες και να μην αφήνουν μεγάλα περιθώρια παραμετροποίησης των συμβατικών όρων[75]. Άλλωστε είναι τέτοια η φύση της τεχνολογίας αυτής που δεν θα επέτρεπε εύκολα τον πάροχο να τροποποιήσει τις λειτουργίες του για να εξυπηρετήσει τις ανάγκες ενός συγκεκριμένου πελάτη. Η χρήση μη διαπραγματεύσιμων τυποποιημένων συμβάσεων συνεπάγεται βέβαια και εξοικονόμηση πόρων για τον πάροχο, συχνά όμως δεν είναι επιθυμητή από τον χρήστη ή τον τελικό καταναλωτή. Συνεπώς, συνίσταται στον πελάτη υπηρεσιών νέφους να μην αναλώνεται τόσο στη διαπραγμάτευση συγκεκριμένων όρων στη

[75] S. Ahmed, Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 6/2014, Ιούνιος 2014.

σύμβαση αλλά να επικεντρώνεται στο να ελέγξει αν οι παρεχόμενες υπηρεσίες εξυπηρετούν τις ανάγκες του και αν ο πάροχος τηρεί διαδικασίες και ελέγχους, συμμορφούμενος για παράδειγμα με πρότυπα και πιστοποιήσεις[76].

5.1.1 Συμφωνίες Επιπέδου Υπηρεσιών (Service Level Agreement-SLA)

Στις συμβάσεις υπολογιστικού νέφους συχνά περιλαμβάνονται και Συμφωνίες Επιπέδου Υπηρεσιών (Service Level Agreement-SLA). Οι SLA είναι όροι της σύμβασης που αφορούν το επίπεδο των παρεχόμενων υπηρεσιών και τον καθορισμό συνεπειών όταν αυτό δεν τηρείται[77]. Έρχονται να συμπληρώσουν τη σύμβαση ως προς το αν παρέχονται εγγυήσεις και αναλαμβάνονται υποχρεώσεις από μέρους του παρόχου για την αδιάλειπτη παροχή υπηρεσιών νέφους χωρίς τεχνικά προβλήματα. Είναι δύσκολο, όμως, να είναι εγγυημένη απόλυτα η απρόσκοπτη λειτουργία του δικτύου και άρα η διαθεσιμότητα των σχετικών υπηρεσιών, γιατί πρόκειται για δίκτυα και μηχανήματα. Ενώ την ίδια στιγμή παραμένει έντονη και η ανησυχία των χρηστών -πελατών για την περίπτωση που δεν θα είναι διαθέσιμες και ακριβείς οι παρεχόμενες συμφωνημένες υπηρεσίες. Μπορεί να υπάρξει απώλεια δεδομένων, θέμα ασφάλειας, αλλά και να υποστούν εν γένει κάποια σχετική ζημιά, η οποία να καθιστά απαραίτητη την καταβολή σε αυτούς αποζημίωσης.

Συνήθως, στις τυποποιημένες συμβάσεις οι πάροχοι ορίζουν στις SLA ότι δεν υπέχουν ευθύνη στην περίπτωση που το σύστημα ή το δίκτυο δεν λειτουργούν και ότι γενικά δεν παρέχουν εγγυήσεις για την αδιάλειπτη λειτουργία των υπηρεσιών τους. Παρολ' αυτά παραμένει αναγκαίο να διασφαλίζεται συμβατικά στις SLA ένα ελάχιστο εγγυημένο από τον πάροχο επίπεδο διαθεσιμότητας και να περιλαμβάνονται ενδεικτικά στοιχεία για τους χρόνους αναμονής, τους όγκους των παρεχόμενων υπηρεσιών, και ταυτόχρονα να ορίζονται συνέπειες όταν δεν τηρούνται. Κάποιοι μεγάλοι πάροχοι προβλέπουν, σε αντίστοιχες SLA που χρησιμοποιούν, οικονομικές

[76] S. Ahmed, Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 6/2014, Ιούνιος 2014.

[77] Αφροδίτη Κουσουνή-Πανταζοπούλου, Νομικές διαστάσεις του Cloud computing, Ψηφιακή Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 2/2012, Απρίλιος - Μάιος - Ιούνιος 2012, σελ.182

επιπτώσεις σε βάρος τους[78], ως κίνητρο για προσέλκυση όλο και περισσότερων πελάτων και ως μέσο πίεσης στους ίδιους για παροχή υψηλού επιπέδου υπηρεσιών.

5.2 Συμβάσεις υπολογιστικού νέφους: νομικός χαρακτηρισμός

Οι συμβάσεις παροχής υπηρεσιών νέφους συνάπτονται εν γένει μέσω διαδικτύου. Ο τύπος και το περιεχόμενο μιας τέτοιας σύμβασης ποικίλει ανάλογα με την τεχνική εκδοχή του νέφους που παρέχεται (SaaS, PaaS, IaaS), και το μοντέλο ανάπτυξης (ιδιωτικό, δημόσιο, κ.λπ.), αλλά και με το αφετέρου συμβαλλόμενο μέρος, που μπορεί να είναι από ένας απλός χρήστης μέχρι ένας πολύ μεγάλος όμιλος επιχειρήσεων.

Συνεπώς, είναι κρίσιμος ο νομικός προσδιορισμός του είδους των συμβάσεων που παρατηρούνται και καταρτίζονται σ' αυτό, έτσι ώστε να απαντηθούν μια σειρά από θέματα μεταξύ των οποίων το εφαρμοστέο δίκαιο και η διεθνής δικαιοδοσία για το σύνολο της εκάστοτε συμβατικής αντιδικίας.

Οι τρεις τεχνικές εκδοχές παροχής υπηρεσιών υπολογιστικού νέφους και τα τέσσερα μοντέλα ανάπτυξης του υπολογιστικού νέφους οδηγούν σε μια μεγάλη ποικιλομορφία. Η μεγάλη ποικιλομορφία, ως προς τις ειδικές ανάγκες και συνθήκες, που καλούνται να καλύψουν κάθε φορά οι καταρτιζόμενες συμβάσεις δυσχεραίνει την υπαγωγή τους σε ένα και μόνον είδος συναπτόμενης σύμβασης. Παρολ' αυτά θα 'ταν επιθυμητό να μπορεί να υπάρξει ένας ενιαίος γενικός χαρακτηρισμός των συμβάσεων αυτών. Η τεχνολογία του υπολογιστικού νέφους είναι ο συνεκτικός κρίκος μεταξύ των διαφορετικών συμβατικών σχέσεων. Με κεντρικό άξονα αυτήν διαμορφώνονται οι υποχρεώσεις και τα δικαιώματα των εμπλεκομένων μερών.

Σύμφωνα με συγκριτική μελέτη[79] στις συμβάσεις υπολογιστικού νέφους εξήχθησαν τα εξής συμπεράσματα:

[78] S. Ahmed, Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ - 6/2014, Ιούνιος 2014, σελ. 12

[79] Ευρωπαϊκή Επιτροπή, Γενική Διεύθυνση Δικαιοσύνης και Καταναλωτών, Συγκριτική μελέτη για συμβάσεις υπολογιστικού νέφους : τελική έκθεση , Υπηρεσία Εκδόσεων, 2015, https://data.europa.eu/doi/10.2838/16333

Οι συμβάσεις υπολογιστικού νέφους μπορεί να περιέχουν στοιχεία από περισσότερα τους ενός είδους των γνωστών συμβατικών τύπων. Η τελική αναφορά της εν λόγω μελέτης στηρίχτηκε στα στοιχεία που ελήφθησαν από τους νομικούς εμπειρογνώμονες που συμμετείχαν, σχετικά με τους νόμους των συμβάσεων που ισχύουν σε σχέση με την πληροφορική (συμπεριλαμβανομένου του cloud computing). Ερευνήθηκαν οι νόμοι των συμβάσεων σε καθένα από τα ευρωπαϊκά κράτη μέλη (εξαιρουμένης της Κροατίας) και στις Η.Π.Α.

Προέκυψε από τη μελέτη ότι όπου υπάρχουν ειδικοί κανόνες για συμβάσεις παροχής υπηρεσιών αυτοί θα μπορούσαν να αποτελέσουν περιεχόμενο των συμβάσεων cloud. Αυτό διαπιστώθηκε για παράδειγμα στη Βουλγαρία, τη Δανία, την Αγγλία και την Ουαλία, την Εσθονία, Φινλανδία, Γαλλία, Ελλάδα, Ιρλανδία, Ιταλία, Λιθουανία, Μάλτα, Πολωνία, Σουηδία, Σλοβενία, Ισπανία και Ολλανδία, αλλά και στις Η.Π.Α. Στη Σουηδία, μάλιστα, συμβάσεις υπολογιστικού νέφους για χωρητικότητα αποθήκευσης, υποδομή ή εφαρμογές τρίτου μέρους θεωρούνται ρητά συμβάσεις υπηρεσιών.

Οι συμβάσεις cloud θα μπορούσαν να εμπίπτουν στους κανόνες των συμβάσεων έργου, για εκείνες τις συμβάσεις όπου ο πάροχος νέφους έχει συμφωνήσει να εκτελεί ορισμένες μόνο εργασίες για τον συγκεκριμένο πελάτη με συγκεκριμένα χαρακτηριστικά προσαρμοσμένα στις ανάγκες αυτού του πελάτη (π.χ. προσαρμογές της υπηρεσίας) όπως έχει αναφερθεί από νομικούς μελετητές στο Βέλγιο, τη Γαλλία, την Ελλάδα, τη Λιθουανία, Λουξεμβούργο, Μάλτα, Σλοβενία και Σουηδία.

Ενδέχεται ακόμη να ισχύουν κανόνες που εφαρμόζονται στις συμβάσεις μίσθωσης, π.χ. σε μοντέλο PaaS, όπου ο πάροχος cloud προσφέρει υπηρεσίες φιλοξενίας που πιθανώς θεωρούνται ως μίσθωση υπολογιστικού χώρου ή σε ένα μοντέλο IaaS όπου μπορεί να θεωρηθεί ότι ο πάροχος cloud μισθώνει υπολογιστική υποδομή στον πελάτη. Είναι, όμως, πιθανό όταν παρέχονται περισσότερες υπηρεσίες από την απλή μίσθωση υπολογιστικού χώρου, να είναι διαφορετικός ο νομικός χαρακτηρισμός.
Αυτό συμβαίνει για παράδειγμα στην Αγγλία & Ουαλία, Ελλάδα, Γαλλία, Ιρλανδία, Ιταλία, Λιθουανία, Λουξεμβούργο, Μάλτα, Πορτογαλία, Ρουμανία, Σουηδία και Σλοβενία.

Παρουσιάζεται ακόμη από Γερμανούς μελετητές ως επικρατούσα στο νομικό δόγμα άποψη η οποία διαχωρίζει μεταξύ μη δωρεάν και δωρεάν συμβάσεων υπολογιστικού νέφους και, γενικά διαφοροποιεί τις κύριες συμβατικές υποχρεώσεις σε μια μη δωρεάν σύμβαση υπολογιστικού νέφους (τόσο SaaS, PaaS όσο και IaaS) και τις εντάσσει σε μια σύμβαση μίσθωσης, όταν βάση της σύμβασης υπολογιστικού νέφους είναι η παροχή υλικού ή/και λογισμικού για περιορισμένο χρονικό διάστημα. Ωστόσο, σημειώνουν ότι αν υπάρχουν πρόσθετες συμβατικές υποχρεώσεις μπορεί να χαρακτηριστεί ως σύμβαση παροχής υπηρεσιών ή/και σύμβαση έργου.

Μια ιδιαίτερη παρατήρηση των Γερμανών μελετητών είναι ότι σε περίπτωση που η σύμβαση συνάπτεται σε δωρεάν βάση, θα μπορούσε να χαρακτηριστεί ως σύμβαση χρησιδανείου.

5.3 Συμβάσεις μίσθωσης ή συμβάσεις παροχής υπηρεσιών

Στη γερμανική νομική επιστήμη φαίνεται αρκετοί να έχουν την άποψη ότι οι συμβάσεις υπολογιστικού νέφους υπάγονται στις συμβάσεις της μίσθωσης. Σύμφωνα με την άποψη αυτή ο προμηθευτής δημιουργεί αφηρημένα υπολογιστικά προϊόντα που μπορούν να χρησιμοποιηθούν από οποιονδήποτε χρήστη. Ο κάθε χρήστης με τη σειρά του αποσκοπεί στο να τα χρησιμοποιήσει και δεν στοχεύει στις υπηρεσίες που ακολουθούν τα υπολογιστικά προϊόντα υπολογιστικού νέφους. Συνεπώς κατά την άποψη αυτή ο χρήστης υπηρεσίας υπολογιστικού νέφους σε οποιοδήποτε μοντέλο παροχής υπηρεσιών (SaaS, PaaS ή IaaS) έχει ανάλογα με τη συνδρομή του το αντίστοιχο χρονικό δικαίωμα χρήσης των σχετικών προϊόντων νεφοϋπολογιστικής έναντι ανταλλάγματος. Με αυτά τα στοιχεία οι συμβάσεις κρίνονται μισθωτικού χαρακτήρα[80].

Φαίνεται, όμως, να λείπει από την παραπάνω άποψη η αξιολόγηση του δυναμικού και πολυσχιδή χαρακτήρα των συμβάσεων νεφοϋπολογιστικής. Ο προμηθευτής αναλαμβάνει τη δημιουργία ενός οικοσυστήματος υπολογιστικών δυνατοτήτων που

[80] Ι. Ρεβολίδης, Διεθνής Δικαιοδοσία και διαδίκτυο, 2020, εκδόσεις Σάκκουλα, σελ. 233-239, Ο νομικός χαρακτηρισμός των συμβάσεων «υπολογιστικού νέφους».

θα καλύπτουν τις ιδιαίτερες ανάγκες και απαιτήσεις κάθε χρήστη. Πέρα από τη δημιουργία όμως αναλαμβάνει τη συνεχή αναβάθμιση και εξέλιξη αυτού του υπολογιστικού οικοσυστήματος που διατηρεί, αλλά παρέχει και την εγγύηση της ασφάλειας και της προστασίας της λειτουργίας του από εξωτερικούς και μη κινδύνους, παρέχοντας την σχετική υποδομή και την αντίστοιχη τεχνική δυνατότητα και λειτουργικότητα. Γίνεται, λοιπόν, εμφανές ότι ο προμηθευτής προϊόντων υπολογιστικού νέφους αναλαμβάνει τη διεκπεραίωση των εκάστοτε υπολογιστικών αναγκών του χρήστη για όλη τη διάρκεια της μεταξύ τους καταρτισθείσας σύμβασης. Επομένως, ο χρήστης έχει μόνο να εκτελέσει την εισαγωγή των δεδομένων που απαιτούνται από αυτόν, ώστε να ολοκληρωθεί η υπολογιστική διαδικασία, ενώ η δημιουργία, η λειτουργία και η ασφάλειά της εξασφαλίζεται από τον προμηθευτή. Ο προμηθευτής παρέχει και συμβουλές καθοδήγησης για τη χρήση των υπηρεσιών του στο λήπτη- χρήστη. Ακολούθως διαμορφώνεται και το αντάλλαγμα που οφείλει να καταβάλει ο χρήστης. Το αντάλλαγμα εξαρτάται από την ποιότητα, τη λειτουργικότητα, τον όγκο και το χρόνο, που χρειάζεται ο κάθε χρήστης. Δημιουργείται έτσι μια μεγάλη ποικιλομορφία, δυναμικά διαμορφωνόμενων συμβάσεων. Γι' αυτό άλλωστε ο προμηθευτής αναλαμβάνει να δημιουργεί ευέλικτες, γεωγραφικά ανεξάρτητες και χρονικά και ποσοτικά προσαρμοζόμενες εφαρμογές υπολογιστικών πόρων, υπολογιστικής δύναμης και ψηφιακής αποθήκευσης. Με αυτά τα χαρακτηριστικά φαίνεται να υπερτερεί ο νομικός χαρακτηρισμός της σύμβασης παροχής υπηρεσιών και ακολούθως μοιάζει δικαιολογημένη η υπαγωγή των συμβάσεων νεφοϋπολογιστικής στον τύπο της σύμβασης παροχής υπηρεσιών του άρθρου 7 (1)(β) του Κανονισμού Βρυξέλλες Ια, δεδομένου ότι ο προμηθευτής των υπηρεσιών αυτών οφείλει να αναλάβει την ενεργό δραστηριότητα της δημιουργίας και της εξασφάλισης της λειτουργικότητας και ασφάλειας των υπολογιστικών εφαρμογών «υπολογιστικού νέφους», προς όφελος του χρήστη των υπηρεσιών, έναντι ανταλλάγματος[81].Τα ανωτέρω επιχειρήματα οδηγούν στην υιοθέτηση της άποψης ότι οι συμβάσεις νεφοϋπολογιστικής είναι συμβάσεις παροχής υπηρεσιών. Η κρίση αυτή δεν πρέπει να κλονίζεται από το στοιχείο της παραχώρησης χρήσης που εμπεριέχεται σε αυτές. Άλλωστε υπάρχει και σχετική απόφαση του ΔΕΕ[82] σύμφωνα με την οποία

[81] Ι. Ρεβολίδης, Διεθνής Δικαιοδοσία και διαδίκτυο, 2020, εκδόσεις Σάκκουλα, σελ. 233-239, Ο νομικός χαρακτηρισμός των συμβάσεων «υπολογιστικού νέφους».

[82] ΔΕΕ C-469/12 (υπόθεση Krejci Lager & Umshlagbetriebs GmbH κατά Olbrich Transport und Logistik GmbH)

το στοιχείο της παραχώρησης χρήσης ακόμη κι όταν υπάρχει δεν χαρακτηρίζει οπωσδήποτε μία σύμβαση. Συγκεκριμένα, η απόφαση αφορούσε το πρόβλημα νομικού χαρακτηρισμού μιας σύμβασης ενσώματων προϊόντων. Το Δικαστήριο έκρινε ότι το κύριο στοιχείο στη σύμβαση αποθήκευσης ενσώματων προϊόντων δεν είναι η παραχώρηση του αποθηκευτικού χώρου, αλλά η ανάληψη της δραστηριότητας της αποθήκευσης, ώστε να δικαιολογείται η ένταξη της στον τύπο της σύμβασης παροχής υπηρεσιών κατά το άρθρο 7(1)(β) του κανονισμού Βρυξέλλες Ια (Καν. 1215/2012). Κατ΄ ανάλογο τρόπο, και στις συμβάσεις νεφοϋπολογιστικής το κύριο στοιχείο είναι ότι ο προμηθευτής που αναλαμβάνει τη διαδικασία διεκπεραίωσης των υπολογιστικών αναγκών του κάθε χρήστη και όχι μόνο την παραχώρηση της χρήσης των υπολογιστικών προϊόντων ή του ψηφιακού αποθηκευτικού χώρου. Δεν διαφοροποιείται ο χαρακτηρισμός της σύμβασης ως σύμβασης παροχής υπηρεσιών ακόμη κι όταν η παραχώρηση χρήσης υπολογιστικών προϊόντων ή του ψηφιακού αποθηκευτικού χώρου αποτελεί μεγάλο μέρος των προσφερόμενων υπηρεσιών αυτό δεν είναι από μόνο του αρκετό για να χαρακτηρίσει τη συμπεριφορά του. Ο προμηθευτής και σε αυτή την περίπτωση εξακολουθεί να μεριμνά για τη συνολική λειτουργία του υπολογιστικού οικοσυστήματος, όπως και για την διαρκή εξέλιξη, συντήρηση, βελτίωση και ασφάλεια αυτού.

Ένα ακόμη στοιχείο που εξετάζεται για τον νομικό χαρακτηρισμό των συμβάσεων νεφοϋπολογιστικής είναι ο τύπος του ανταλλάγματος που καταβάλει ο λήπτης των υπηρεσιών νεφοϋπολογιστικής. Δεν θα πρέπει όμως να επηρεαστεί ο χαρακτηρισμός των σχετικών συμβάσεων ως συμβάσεων παροχής υπηρεσιών ούτε στην εξαιρετικά συχνή περίπτωση κατά την οποία ο λήπτης των υπηρεσιών αυτών παραχωρεί προσωπικά δεδομένα ως αντάλλαγμα για τις υπηρεσίες που λαμβάνει, καθώς δεν αμφισβητείται ο αμφοτεροβαρής χαρακτήρας των συμβάσεων. Το ΔΕΕ ενδεικτικά στις υποθέσεις C-9/12 (Corman Collins κατά La Maison du Whisky),παρ.39-40, και ΔΕΕ C-196/15(Granarolo SpA κατά Ambrosi Emmi France SA), παρ.40-41, έχει αποφανθεί ότι «η αντιπαροχή που οφείλει ο λήπτης των υπηρεσιών δε χρειάζεται να έχει χρηματική μορφή, αλλά δύναται να λαμβάνει την μορφή ανταγωνιστικών πλεονεκτημάτων, αρκεί αυτά να έχουν οικονομική αξία για τον παρέχοντα τις υπηρεσίες». Συνεπώς, σημασία έχει η οικονομική αξία της αντιπαροχής, ανεξάρτητα από την χρηματική ή μη μορφή της, και εφόσον αυτή υπάρχει, κρίνεται η σύμβαση ως σύμβαση παροχής υπηρεσιών και εφαρμόζεται το άρθρο 7(1)(β) του κανονισμού

Βρυξέλλες Ια (Καν. 1215/2012). Βασική φιλοσοφία του άρθρου αυτού είναι η συγκέντρωση όλων των διαφορών των προερχόμενων από τη σύμβαση ενώπιον των δικαστηρίων του οικονομικού κέντρου μιας σύμβασης «έτσι όπως αυτό εκφράζεται στον τόπο εκπλήρωσης της χαρακτηριστικής παροχής, ανεξάρτητα και χωρίς να λαμβάνεται υπόψη ο τόπος εκπλήρωσης της αντιπαροχής»[83].

5.4 Διεθνής δικαιοδοσία στις συμβάσεις υπολογιστικού νέφους ως συμβάσεις παροχής υπηρεσιών

Εφαρμογή του άρθρου 7(1)(β) του κανονισμού Βρυξέλλες Ια στις συμβάσεις παροχής υπηρεσιών

Βάσει του άρθρου 7(1)(β) του κανονισμού Βρυξέλλες Ια (Καν. 1215/2012) προβλέπεται : «Πρόσωπο που έχει την κατοικία του σε κράτος μέλος μπορεί να εναχθεί σε άλλο κράτος μέλος: 1. β) για τους σκοπούς της εφαρμογής της παρούσας διάταξης, και εφόσον δεν συμφωνήθηκε διαφορετικά, ο τόπος εκπλήρωσης της επίδικης παροχής είναι: — εφόσον πρόκειται για πώληση εμπορευμάτων, ο τόπος του κράτους μέλους όπου, δυνάμει της σύμβασης, έγινε ή έπρεπε να γίνει η παράδοση των εμπορευμάτων, — εφόσον πρόκειται για παροχή υπηρεσιών, ο τόπος του κράτους μέλους όπου, δυνάμει της σύμβασης, έγινε ή έπρεπε να γίνει η παροχή των υπηρεσιών·» και το άρθρο 7 παρ.1 συνεχίζεται με το στοιχείο γ. που προβλέπει: «το στοιχείο α) εφαρμόζεται, εφόσον δεν εφαρμόζεται το στοιχείο β)·».

Σύμφωνα με όλα τα ανωτέρω οι συμβάσεις υπολογιστικού νέφους κρινόμενες ως συμβάσεις παροχής υπηρεσιών θα ακολουθήσουν για τον εντοπισμό του τόπου εκπλήρωσης της παροχής το άρθρο 7 παρ. 1 στοιχείο β του Κανονισμού Βρυξελλών Ια. Κατά την εφαρμογή αυτού του άρθρου, για να εντοπιστεί ο τόπος εκπλήρωσης της παροχής των υπηρεσιών, θα εξεταστεί αρχικά αν με κάποιο όρο της ίδιας της σύμβασης έχει προσδιοριστεί ρητά ο τόπος εκπλήρωσης της παροχής των υπηρεσιών ή αν

[83] Ι. Ρεβολίδης, Διεθνής Δικαιοδοσία και διαδίκτυο, 2020, εκδόσεις Σάκκουλα, σελ. 233-239, Ο νομικός χαρακτηρισμός των συμβάσεων «υπολογιστικού νέφους».

περιέχονται ισχυρά στοιχεία από τα οποία συνάγεται. Αν δεν προκύψει ο τόπος εκπλήρωσης της παροχής των υπηρεσιών από τη σύμβαση, τότε πρέπει εν αμφιβολία να αναζητηθεί στον τόπο εγκατάστασης του παρέχοντος τις υπηρεσίες. Μια τέτοια προσέγγιση είναι σύμφωνη με τον πραγματολογικό χαρακτήρα του δικαιοδοτικού κριτηρίου του άρθρου 7 (1)(β) και το τεκμήριο ότι ο παρέχων τις υπηρεσίες οργανώνει την παροχή τους στον τόπο της κύριας εγκατάστασης του[84]. Συνεπώς, θα πρέπει να ερευνάται και να εντοπίζεται η γεωγραφική διάταξη του παρόχου όπου γίνεται η μεγαλύτερη ποιοτικά δέσμευση των πόρων του, των απαραίτητων για την εκτέλεση της εκάστοτε σύμβασης[85]. Ο εντοπισμός αυτός οδηγεί συχνά στην έδρα του παρόχου των υπηρεσιών υπολογιστικού νέφους, αφού εκεί βασικά οργανώνει την παροχή των υπηρεσιών του και εγκαθιστά κι αξιοποιεί την υλικοτεχνική υποδομή του, κυρίως στις περιπτώσεις που ο πάροχος έχει μια απλή διάταξη υπολογιστικών δραστηριοτήτων. Στις περιπτώσεις που μοιράζεται η δραστηριότητά του μεταξύ περισσότερων κρατών μελών, θα πρέπει να εντοπίζεται ως τόπος εγκατάστασης του παρόχου ο τόπος των κύριων δραστηριοτήτων οργάνωσης και εκτέλεσης των εν λόγω υπηρεσιών, με ενδεικτικά κριτήρια τους πόρους, τις τεχνικές γνώσεις, το προσωπικό και το χρόνο που αφιερώνει και χρησιμοποιεί σε κάθε διάταξη. Όταν το τελευταίο είναι δυσχερές, ως λύση προκρίνεται η έδρα του παρόχου, που αποτελεί άλλωστε τον κύριο χώρο εκδήλωσης των επιχειρηματικών του δραστηριοτήτων. Η έδρα του παρόχου ως δικαιοδοτικό κριτήριο οδηγεί στην υλοποίηση του πραγματολογικού δεσμού μεταξύ του δικαστηρίου που δικάζει και της επίδικης διαφοράς και δίνει λύση στα προβλήματα που δημιουργούν οι τεχνολογικές ιδιαιτερότητες του διαδικτύου. Εγγυάται ακόμη ότι θα ληφθούν υπόψει «οι τεχνικές, οικονομικές και εν γένει οργανωτικές περιστάσεις που χαρακτηρίζουν τον τρόπο λειτουργίας του υπολογιστικού συστήματος «υπολογιστικού νέφους» που διατηρεί ο πάροχος». Δίνεται έτσι η δυνατότητα και στον πάροχο και στον λήπτη των υπηρεσιών να αποδείξουν καλύτερα τους ισχυρισμούς τους έχοντας πρόσβαση στην κρίσιμη οργανωτική δομή του παρόχου.

Με αυτή τη δικαιοδοτική επιλογή της εφαρμογής του άρθρου 7 (1) (β) του Κανονισμού Βρυξελλών Ια στις συμβάσεις υπολογιστικού νέφους αποφεύγεται η δυνατότητα του

[84] Ι. Ρεβολίδης, Διεθνής δικαιοδοσία και διαδίκτυο,2020, εκδόσεις Σάκκουλα, σελ.260-266, «Ο προσδιορισμός του τόπου εκπλήρωσης της παροχής στην περίπτωση των συμβάσεων παροχής «υπολογιστικού νέφους».

[85] Βλ. Ανωτέρω υποσημείωση υπ' αρ. 84.

λήπτη να καταστρατηγήσει τους δικαιοδοτικούς κανόνες επιλέγοντας γεωγραφικά αυθαίρετα και τυχαία το δικαιοδοτικό κέντρο της αντιδικίας. Χαρακτηριστικό της τεχνολογίας του υπολογιστικού νέφους είναι η διάσπαση της υπολογιστικής δύναμης γεωγραφικά οπουδήποτε. Αυτό θα έδινε το περιθώριο στο λήπτη αν κρίσιμος ήταν ο τόπος όπου αυτός λαμβάνει τις υπηρεσίες, να επέλεγε να κάνει χρήση των υπηρεσιών από οπουδήποτε στον κόσμο, με κίνδυνο να μην υπάρχει εγγύτητα και συνάφεια των δικαστηρίων που θα προσδιορίζονταν με τη διαφορά και ο πάροχος να μην μπορεί να προφυλαχθεί «από το ενδεχόμενο να εναχθεί σε μία από τις περισσότερες χώρες όπου εκπληρώνεται σημαντικό μέρος της παροχής»[86,87].

[86] Βλ. ΔΕΕ υπόθεση C-19/09 (Wood Floor Solutions κατά Silva Trade SA).

[87] Βλ. σχόλιο Ευάγγελου Βασιλακάκη στην υπόθεση ΔΕΕ υπόθεση C-19/09 (Wood Floor Solutions κατά Silva Trade SA), ΕΠολΔ 2010, σελ. 463, ιδίως 467.

6 Ασφάλεια δεδομένων στο υπολογιστικό νέφος

Η ασφάλεια στο υπολογιστικό νέφος είναι δύσκολο να επιτευχθεί, ακριβώς λόγω του ανοιχτού του περιβάλλοντος, της πολυδιάστατης δομής του και του «ατοπικού» του χαρακτήρα και απαιτεί καταρχήν ένα μείγμα τεχνολογιών, τεχνικών ρυθμίσεων και συμπεριφορών, με στόχο την ακεραιότητα των συστημάτων και κατ' επέκταση των δεδομένων. Από τη στιγμή που ο χρήστης αποθηκεύσει τα δεδομένα του στο cloud, κάπου δηλαδή ανά τον κόσμο, πρακτικά χάνει ο ίδιος τον έλεγχό τους και τα "εμπιστεύεται" σε κάποιον τρίτο– πιθανόν τον πάροχο. Έτσι, ο "ιδιοκτήτης" των προσωπικών δεδομένων είναι διαφορετικό πρόσωπο από τον "φύλακα" αυτών .Στην υπολογιστική νέφους τα δεδομένα αποθηκεύονται σε διαφορετικές γεωγραφικές τοποθεσίες που έχουν διαφορετικές νομικές δικαιοδοσίες. Εξαιτίας του multi-tenant περιβάλλοντος πολλοί χρήστες μπορούν να αποθηκεύσουν τα δεδομένα τους στην ίδια τοποθεσία χρησιμοποιώντας φυσική ή εικονική αποθήκευση. Έτσι μπορεί ένας χρήστης να εισβάλει σε δεδομένα τοποθεσίας άλλου χρήστη. Τα περισσότερα ζητήματα ασφάλειας οφείλονται σε τρωτά σημεία στην εικονική απεικόνιση, την αποθήκευση και το δίκτυο, τα οποία είναι επίσης σημαντικοί παράγοντες της τεχνολογίας υπολογιστικού νέφους.

Τα στάδια «ζωής» των δεδομένων είναι έξι[88]: 1. Δημιουργία, 2. αποθήκευση, 3. χρήση, 4. μεταφορά, 5.αρχειοθέτηση, 6. καταστροφή. Αφού δημιουργηθούν τα δεδομένα, μπορούν ελεύθερα να κυκλοφορούν μεταξύ των σταδίων. Τα δεδομένα θα πρέπει να είναι ασφαλή σε όλο τον «κύκλο της ζωής» τους από την δημιουργία μέχρι την καταστροφή τους. Τα στάδια αποθήκευσης και αρχειοθέτησης ονομάζονται «δεδομένα σε ξεκούραση» (data-at-rest), το στάδιο χρήσης ονομάζεται «δεδομένα σε χρήση» (data-in-use), το στάδιο μεταφοράς ονομάζεται «δεδομένα σε διαβίβαση» (data-in-transit), ενώ το στάδιο καταστροφής αποκαλείται «δεδομένα μετά τη διαγραφή» (data-after-delete)[89].

[88] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science 125, page 691-697(page 693).
[89] Βλ. Ανωτέρω υποσημείωση υπ' αρ. 88.

6.1 Το τρίπτυχο CIA

Ένα ασφαλές υπολογιστικό νέφος, πρέπει πρώτα απ' όλα να διακρίνεται από το τρίπτυχο CIA (Confidentiality-Integrity-Availability), να διακρίνεται δηλαδή από τα εξής χαρακτηριστικά[90]:

i) την εμπιστευτικότητα (Confidentiality) : Αυτή διασφαλίζει ότι τα δεδομένα που στέλνονται μπορεί να τα δει αποκλειστικά και μόνο ένας εξουσιοδοτημένος–εγκεκριμένος χρήστης και εξ' αντιδιαστολής περιορίζεται η πρόσβαση σε κακόβουλα τρίτα μέρη στα δεδομένα που διακινούνται ή βρίσκονται αποθηκευμένα σε αυτό. Η κρυπτογράφηση των προσωπικών δεδομένων θα πρέπει να χρησιμοποιείται σε όλες τις περιπτώσεις κατά την «διαμετακόμιση» αλλά και όταν είναι διαθέσιμα τα δεδομένα «σε κατάσταση ηρεμίας». Πρέπει να δίνεται ιδιαίτερη προσοχή στη διαχείριση κρυπτογραφικών κλειδιών καθώς η ασφάλεια των δεδομένων εξαρτάται τελικά και συνδέεται με την εμπιστευτικότητα των κλειδιών κρυπτογράφησης.

Οι επικοινωνίες μεταξύ παρόχου και πελάτη καθώς και μεταξύ κέντρων δεδομένων θα πρέπει να γίνονται κρυπτογραφημένα. Η απομακρυσμένη διαχείριση της πλατφόρμας cloud θα πρέπει να πραγματοποιείται μόνο μέσω καναλιού ασφαλούς επικοινωνίας. Εάν ένας πελάτης σκοπεύει όχι μόνο να αποθηκεύσει, αλλά και να επεξεργαστεί περαιτέρω τα προσωπικά του δεδομένα στο cloud (π.χ. αναζήτηση σε βάσεις δεδομένων για εγγραφές), πρέπει να έχει υπόψη του ότι η κρυπτογράφηση δεν μπορεί να διατηρηθεί κατά την επεξεργασία των δεδομένων (εκτός από πολύ συγκεκριμένους υπολογισμούς).

Περαιτέρω τεχνικά μέτρα που αποσκοπούν στη διασφάλιση του απορρήτου περιλαμβάνουν την έγκριση μηχανισμών και ισχυρό έλεγχο ταυτότητας (π.χ. έλεγχος ταυτότητας δύο παραγόντων). Υποχρεώσεις εμπιστευτικότητας πρέπει να επιβάλλονται στους υπαλλήλους των πελατών cloud, των παρόχων cloud και των υπεργολάβων με συμβατικές ρήτρες.

[90] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science 125, page 691-697(page 693-694).

ii) την ακεραιότητα (Integrity): ήτοι τη διασφάλιση ότι τα δεδομένα που έστειλε ο χρήστης προς την υπηρεσία του νέφους, έφθασαν σε αυτήν ακέραια και όχι τροποποιημένα από κάποιον μη εξουσιοδοτημένο. Η ακεραιότητα των δεδομένων αφορά στη διαπίστωση μιας κακόβουλης τροποποίησης αυτών, χωρίς ωστόσο να συμπεριλαμβάνει και την έννοια της πρόληψης αυτής (της τροποποίησης).

Μηχανισμοί κρυπτογραφικής πιστοποίησης μπορούν να βοηθήσουν στην κατεύθυνση του εντοπισμού αλλαγών στα προσωπικά δεδομένα, ηλεκτρονικοί κωδικοί ή οι ηλεκτρονικές υπογραφές ελέγχου γνησιότητας μηνύματος. Ακόμη μέσα ανίχνευσης εισβολών / συστημάτων πρόληψης (IPS / IDS) μπορούν να αποτρέψουν κακόβουλες επεμβάσεις στην ακεραιότητα των συστημάτων πληροφορικής στο cloud. «Αυτό είναι ιδιαίτερα σημαντικό στον τύπο του περιβάλλοντος ανοιχτού δικτύου στο οποία συνήθως λειτουργούν τα σύννεφα».

iii) τη διαθεσιμότητα (Availability): σημαίνει διασφάλιση έγκαιρης και αξιόπιστης πρόσβασης στα προσωπικά δεδομένα.
Μια σοβαρή απειλή για τη διαθεσιμότητα στο cloud είναι η τυχαία απώλεια της συνδεσιμότητας δικτύου μεταξύ του πελάτη και του παρόχου ή της απόδοσης του διακομιστή που προκαλείται από κακόβουλες ενέργειες όπως επιθέσεις (κατανεμημένης) άρνησης υπηρεσίας (DoS). Άλλοι κίνδυνοι διαθεσιμότητας περιλαμβάνουν τυχαίες αστοχίες του υλισμικού τόσο στο δίκτυο όσο και στα συστήματα επεξεργασίας και αποθήκευσης δεδομένων στο cloud, διακοπές ρεύματος και άλλα προβλήματα υποδομής.

Οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει να ελέγχουν εάν ο πάροχος cloud έχει λάβει εύλογα μέτρα για να αντιμετωπίσει τον κίνδυνο διαταραχών, όπως εφεδρικές συνδέσεις δικτύου στο Διαδίκτυο, πλεονάζουσα αποθήκευση και αποτελεσματικούς μηχανισμούς δημιουργίας αντιγράφων ασφαλείας δεδομένων.

Περαιτέρω για ένα ασφαλές υπολογιστικό σύννεφο θα πρέπει να υπάρχει αυθεντικότητα: χαρακτηριστικό το οποίο εγγυάται ότι κάτι παρέχεται από μία εξουσιοδοτημένη πηγή - την αυθεντική, χωρίς δυνατότητα άρνησης ή αμφισβήτησης μιας προηγούμενης δέσμευσης ή πράξης (μη υπαναχώρηση) σε κάποιο τρίτο μέρος. Αποτελεί σημαντικό χαρακτηριστικό, ειδικά για τις περιπτώσεις

που υπάρχει μία διαφωνία σχετική με την ανταλλαγή δεδομένων. Άλλα χαρακτηριστικά όπως η διαφάνεια, που έχει αναφερθεί και ανωτέρω, η πιστοποίηση ως απόδειξη ότι το άτομο θα έχει πρόσβαση στα δικά του δεδομένα(οι χρήστες πρέπει να πιστοποιούνται πριν διεξάγουν κάποια δραστηριότητα για την οποία έχουν την άδεια), και η πρόσβαση ελέγχου στα δεδομένα, είναι χαρακτηριστικά που μπορούν να συμβάλουν στην ασφάλεια στο σύννεφο[91].

[91] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691-697.

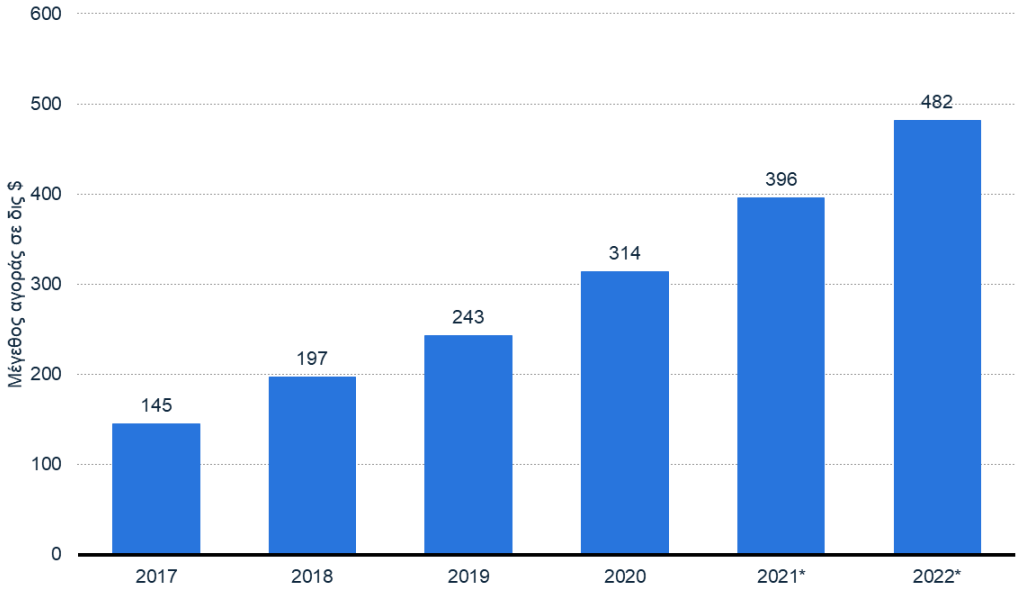
7 Οικονομικές διαστάσεις της χρήσης υπηρεσιών υπολογιστικού νέφους

7.1 Εισαγωγή

Ένας από τους πρωταρχικούς στόχους των επιχειρήσεων είναι η μεγιστοποίηση της αξίας τους. Προς αυτή την κατεύθυνση μπορεί να συμβάλει μεταξύ άλλων και ο περιορισμός των λειτουργικών εξόδων τους. Αυτός φαίνεται να είναι και ένας από τους σημαντικότερους λόγους χρήσης υπηρεσιών υπολογιστικού νέφους από τις επιχειρήσεις και τους οργανισμούς. Σε αυτό το κεφάλαιο εξετάζουμε τους παράγοντες που επηρεάζουν την απόφαση για τη χρήση ή μη υπηρεσιών υπολογιστικούς νέφους, αλλά και πως θα πρέπει να γίνεται η επιλογή της κατάλληλης υπηρεσίας.

7.2 Εξέλιξη της αγοράς υπηρεσιών υπολογιστικού νέφους

Τα τελευταία χρόνια η ζήτηση για υπηρεσίες υπολογιστικού νέφους διαρκώς αυξάνεται. Ειδικότερα, η παγκόσμια αγορά δημόσιου υπολογιστικού νέφους αναπτύσσεται διαρκώς και αναμένεται να φτάσει τα 482 δισεκατομμύρια δολάρια το 2022.

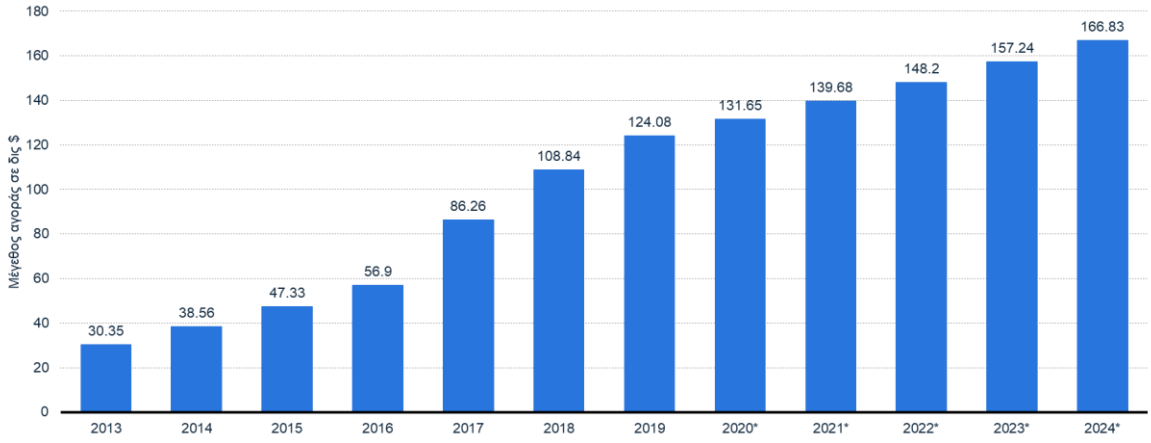


Διάγραμμα 1: Μέγεθος παγκόσμιας αγοράς δημόσιου υπολογιστικού νέφους 2017 – 2022

Πηγή: gartner.com

Η υψηλή ζήτηση υπηρεσιών δημόσιου υπολογιστικού νέφους οφείλεται στο ότι είναι οικονομικά αποδοτικές. Συγκεκριμένα, οι υπηρεσίες προσφέρονται στον πελάτη μέσω ενός μοντέλου πληρωμής ανάλογα με τη χρήση (pay-as-you-go). Αυτό σημαίνει ότι δεν πρέπει να γίνουν προκαταβολικές επενδύσεις που διαφορετικά οδηγούν σε λειτουργικά κόστη για τη συντήρηση του υλικού και της υποδομής εφαρμογών εσωτερικής εγκατάστασης. Αντίθετα, ο πάροχος υπηρεσιών υπολογιστικού νέφους διασφαλίζει τη σωστή διαχείριση και συντήρηση του συστήματος και ο πελάτης πληρώνει μόνο για τις υπηρεσίες που καταναλώνει.

Ανάλογη είναι και η ανάπτυξη της αγοράς εφαρμογών που βασίζονται σε υπηρεσίες υπολογιστικού νέφους. Το 2019, η παγκόσμια αγορά εφαρμογών υπολογιστικού νέφους είχε αξία 124,1 δισεκατομμυρίων δολαρίων και αναμένεται να φτάσει τα 166,8 δισεκατομμύρια δολάρια έως το 2024. Η αγορά λογισμικού εφαρμογών υπολογιστικού νέφους αναμένεται να αναπτυχθεί με ένα σύνθετο ετήσιο ρυθμό ανάπτυξης 6,1% σύμφωνα με τις προβλέψεις της Apps Run The World.



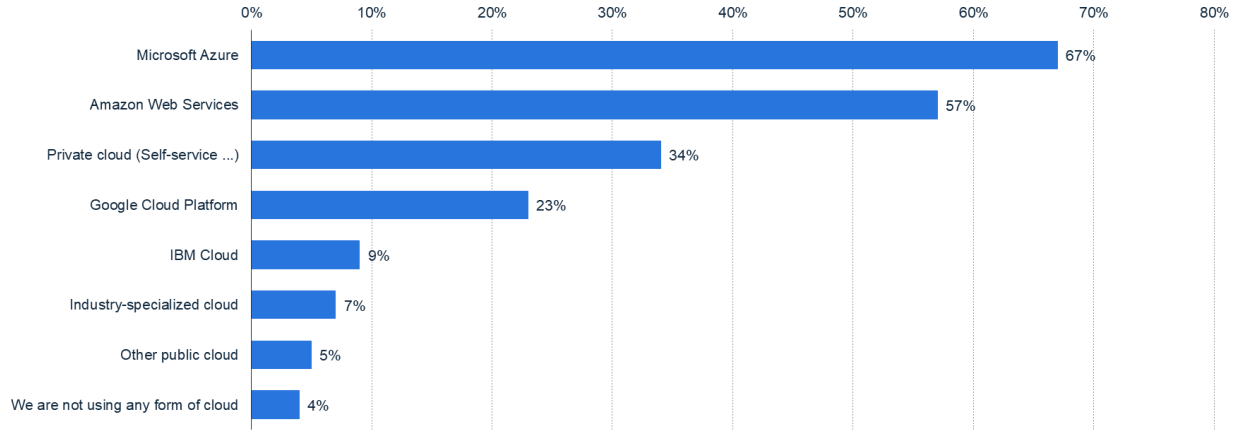
Διάγραμμα 2: Παγκόσμια αγορά εφαρμογών υπολογιστικού νέφους 2013-2024

Πηγή: Apps Run The World; appsruntheworld.com

Όσον αφορά τη δημοτικότητα των παρόχων υπηρεσιών δημόσιου υπολογιστικού νέφους ξεχωρίζουν η Microsoft Azure, η Amazon Web Services (AWS) και η Google Cloud. Σύμφωνα με έρευνα της Turbonomic που πραγματοποιήθηκε[92] τον Φεβρουάριο του 2021, το 67% των ερωτηθέντων δήλωσαν ότι χρησιμοποιούν το Microsoft Azure

[92] Συμμετείχαν στην έρευνα 819 ειδικοί πληροφορικής σε εταιρίες από μικρές μέχρι πολυεθνικές σε διάφορους κλάδους

για τις υπηρεσίες υπολογιστικού νέφους τους. Μέχρι το 2020 η Amazon Web Services (AWS) ήταν στην κορυφή της λίστας, όταν η Microsoft πήρε τη θέση της. Χαρακτηριστικό επίσης είναι, ότι το ποσοστό των ερωτηθέντων που δεν χρησιμοποιούσαν καμία μορφή υπηρεσιών υπολογιστικού νέφους μειώθηκε στο 4% το 2021 από 8% που ήταν το 2020. Η προτίμηση αυτών των παρόχων δεν είναι τυχαία. Αυτές οι εταιρίες έχουν αναπτύξει μια παγκόσμια υποδομή υπηρεσιών υπολογιστικού νέφους διασφαλίζοντας υψηλά πρότυπα ασφάλειας και επιτυγχάνοντας μεγάλα επίπεδα αξιοπιστίας. Από το διάγραμμα 3 παρατηρούμε επίσης ότι η χρήση ιδιωτικού υπολογιστικού νέφους καταλαμβάνει την τρίτη θέση.



Διάγραμμα 3: Χρήση υπηρεσιών υπολογιστικού νέφους από επιχειρήσεις παγκοσμίως το 2021, ανά πάροχο.
Πηγή: Turbonomic

Σε αντίθεση με άλλους κλάδους, η αγορά υπηρεσιών δημόσιου υπολογιστικού νέφους φαίνεται να επηρεάζεται θετικά τόσο άμεσα όσο και μακροπρόθεσμα από την πανδημία Covid-19. Η υγειονομική κρίση ανέδειξε τα οφέλη των υπηρεσιών υπολογιστικού νέφους τόσο στα πλαίσια της τηλεργασίας όσο και σε θέματα ευελιξίας των επιχειρηματικών διαδικασιών ιδίως σε περιόδους κρίσης. Η πανδημία οδήγησε σε ταχεία υιοθέτηση από επιχειρήσεις και οργανισμούς υπηρεσιών υπολογιστικού νέφους αυξάνοντας έτσι τα έσοδα του κλάδου.

7.3 Πλεονεκτήματα και προκλήσεις της χρήσης υπηρεσιών υπολογιστικού νέφους

Η χρήση υπηρεσιών υπολογιστικού νέφους από τις επιχειρήσεις και οργανισμούς έχει τα παρακάτω πλεονεκτήματα:

7.3.1 Κόστος

Η χρησιμοποίηση υπηρεσιών υπολογιστικού νέφους δεν απαιτεί η επιχείρηση να επενδύσει σε υλικό. Έτσι μπορεί να γίνει καλύτερη διαχείριση των διαθέσιμων οικονομικών πόρων της καθώς η επιχείρηση πληρώνει μόνο για τις υπηρεσίες και το χώρο που χρησιμοποιεί κάθε φόρα.

7.3.2 Ευελιξία

Οι τεχνολογίες υπολογιστικού νέφους είναι τυποποιημένες σε όλες τις τοποθεσίες και έτσι επιτρέπουν την κινητικότητα, βελτιώνοντας τη συνεργασία και την κοινή χρήση.

7.3.3 Καινοτομία

Οι υπηρεσίες υπολογιστικού νέφους δίνουν τη δυνατότητα στις επιχειρήσεις να πραγματοποιήσουν άμεσα αναβαθμίσεις και καινοτομίες σε υπάρχοντα ή νέα προϊόντα.

7.3.4 Επεκτασιμότητα

Οι υπηρεσίες υπολογιστικού νέφους δίνουν τη δυνατότητα στις επιχειρήσεις να αυξάνουν ή να μειώνουν γρήγορα τη χωρητικότητα που έχουν στη διάθεση τους ανάλογα με τις ανάγκες τους. Με αυτόν τον τρόπο, μεγιστοποιείται η αξιοποίηση της διαθέσιμης χωρητικότητας.

7.3.5 Συντήρηση

Οι υπηρεσίες υπολογιστικού νέφους διαχειρίζονται από τρίτους και συνεπώς δεν απαιτείται συντήρηση από τον πελάτη.

7.3.6 Ασφάλεια

Το λογισμικό ενημερώνεται αυτόματα από τον πάροχο υπηρεσιών υπολογιστικού νέφους για διορθώσεις σφαλμάτων και επικαιροποίηση έναντι διαδικτυακών απειλών.

Ενδιαφέρον παρουσιάζουν τα αποτελέσματα του Statista Global Consumer Survey, 2020, όσον αφορά τα μεγαλύτερα οφέλη που θεωρούν ότι αποκομίζουν οι χρήστες υπηρεσιών υπολογιστικού νέφους σε Ηνωμένες Πολιτείες Αμερικής, Ηνωμένο Βασίλειο και Γερμανία. Σύμφωνα με αυτή την έρευνα η ασφάλεια των δεδομένων αναφέρεται ως το μεγαλύτερο όφελος από όλους τους συμμετέχοντες. Ακολουθεί η μεγαλύτερη χωρητικότητα αποθήκευσης ιδίως για τους συμμετέχοντες από Ηνωμένες Πολιτείες Αμερικής και Ηνωμένο Βασίλειο. Οι συμμετέχοντες στην έρευνα από τη Γερμανία αξιολογούν ως επίσης σημαντική τη δυνατότητα χρήσης δεδομένων από διαφορετικές συσκευές και διαφορετικές τοποθεσίες. Τέλος, άλλο ένα σημαντικό όφελος που αναφέρεται από το σύνολο των συμμετεχόντων είναι ότι οι υπηρεσίες υπολογιστικού νέφους διευκολύνουν την κοινή χρήση δεδομένων μεταξύ ατόμων.

Εκτός από τα οφέλη που προσφέρει στις επιχειρήσεις και οργανισμούς η χρήση υπηρεσιών υπολογιστικού νέφους συνεπάγεται και κάποιες προκλήσεις η διαχείριση των οποίων μπορεί να αποτελεί και αποτρεπτικό παράγοντα για την μετάβαση του συνόλου των διεργασιών μιας επιχείρησης στο υπολογιστικό νέφος.

7.3.7 Θέματα συμμόρφωσης με κανονιστικά πλαίσια

Μια από τις προκλήσεις της χρήσης υπολογιστικού νέφους είναι η συμμόρφωση της επιχείρησης με σχετικά κανονιστικά πλαίσια (π.χ. Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR). Προκειμένου μια επιχείρηση ή ένας οργανισμός να μεταφέρει τα δεδομένα που διαχειρίζεται από τους προσωπικούς του χώρους αποθήκευσης (π.χ. τοπικούς servers) στο υπολογιστικό νέφος θα πρέπει προηγουμένως να εξετάσει ότι αυτό γίνεται λαμβάνοντας υπόψη την ισχύουσα νομοθεσία.

7.3.8 Διαχείριση υπολογιστικού νέφους

Άλλη μια πρόκληση είναι η διαχείριση των δαπανών που κάνει μια επιχείρηση για χρήση υπηρεσιών υπολογιστικού νέφους. Προκειμένου να επωφεληθεί η επιχείρηση από αυτή την υπηρεσία θα πρέπει το οικονομικό τμήμα της να έχει την κατάλληλη εξειδίκευση για να διαχειρίζεται και να προγραμματίζει τις δαπάνες για χρήση υπηρεσιών υπολογιστικού νέφους ανάλογα με τις ανάγκες κάθε φορά.

7.3.9 Θέματα κυβερνοασφάλειας

Ο βαθμός κυβερνοασφάλειας είναι άλλη μια πρόκληση στη χρήση υπηρεσιών υπολογιστικού νέφους. Ορισμένες εταιρείες είναι επιφυλακτικές ως προς το βαθμό ασφάλειας που παρέχουν τα δημόσια υπολογιστικά νέφη, επιλέγοντας να αποθηκεύουν σε αυτά όχι και τόσο εμπιστευτικά δεδομένα.

7.3.10 Ενδεχόμενη πολυπλοκότητα της διαδικασίας μετάβασης των δεδομένων στο υπολογιστικό νέφος

Σε ορισμένες περιπτώσεις μπορεί να υπάρξουν δυσκολίες κατά τη μεταφορά των δεδομένων από τους τοπικούς πόρους μιας επιχείρησης στο υπολογιστικό νέφος. Όσο μεγαλύτερη η επιχείρηση ή ο όγκος και η διαφορετικότητα των χαρακτηριστικών των δεδομένων, τόσο μεγαλύτερος και ο βαθμός πολυπλοκότητας της συγκεκριμένης διαδικασίας.

7.3.11 Έλλειψη τεχνογνωσίας

Η εκπαίδευση των εργαζομένων της επιχείρησης στη χρήση των υπηρεσιών υπολογιστικού νέφους αποτελεί άλλη μια πρόκληση την οποία θα πρέπει να διαχειριστούν όσοι επιλέγουν τη χρήση αυτών των υπηρεσιών.

7.4 Διαδικασία λήψης απόφασης για χρήση υπηρεσιών υπολογιστικού νέφους

Παρά τα πλεονεκτήματα του υπολογιστικού νέφους, η υιοθέτηση και η ενσωμάτωση των υπηρεσιών του με τα υπάρχοντα παραδοσιακά συστήματα μιας επιχείρησης, μπορεί να δημιουργήσει σημαντικά εμπόδια. Αυτές οι προκλήσεις μπορεί να προκύψουν σε διαφορετικούς τομείς, συμπεριλαμβανομένης της νομοθεσίας, της

στρατηγικής διαχείρισης και της τεχνολογίας ιδίως όσον αφορά θέματα κυβερνοασφάλειας[93].

Συνεπώς, ο προγραμματισμός και ο σχεδιασμός του τρόπου με τον οποίο τα δεδομένα και οι εφαρμογές που χρησιμοποιεί μια επιχείρηση για τις δραστηριότητες της θα μεταφερθούν στο υπολογιστικό νέφος, αποτελεί ένα σημαντικό μέρος των στρατηγικών που αναπτύσσει το τμήμα πληροφορικής της επιχείρησης και απαιτεί συστηματική προσέγγιση. Μία επιχείρηση προτού προχωρήσει στη χρήση αυτών των υπηρεσιών θα πρέπει σύμφωνα με τους Kaisler *et al* (2012)[94] να δώσει απαντήσεις στα ακόλουθα ερωτήματα:

- Πότε, πώς και πόσες διεργασίες πρέπει να μεταφερθούν στο υπολογιστικό νέφος;
- Πώς θα γίνει η διαχείριση των κεφαλαιουχικών και λειτουργικών εξόδων που σχετίζονται με τη χρήση υπηρεσιών υπολογιστικού νέφους;
- Ποιος είναι ο βέλτιστος συνδυασμός υπηρεσιών υπολογιστικού νέφους και πώς θα επιτευχθεί;
- Πώς διασφαλίζει η επιχείρηση ότι ο πάροχος υπηρεσιών υπολογιστικού νέφους συμμορφώνεται με την εφαρμογή κανονισμών και νόμων διαχείρισης προσωπικών δεδομένων;
- Πώς θα ελέγχει η επιχείρηση τη ροή των δεδομένων από και προς το περιβάλλον υπολογιστικού νέφους και τα στοιχεία αρχιτεκτονικής του συστήματος;

Για να γίνει η μετάβαση στο υπολογιστικό νέφος, η επιχείρηση θα πρέπει να ακολουθήσει τα εξής στάδια:

7.4.1 Αξιολόγηση

Τα στελέχη και οι υπεύθυνοι λήψης αποφάσεων πληροφορικής πρέπει να αξιολογήσουν τις ευκαιρίες και τις προκλήσεις της εφαρμογής μιας στρατηγικής υπολογιστικού νέφους για τα χαρακτηριστικά της επιχείρησης τους. Θα πρέπει να

[93] Alassafi, M. O., AlGhamdi, R., Alshdadi, A., Al Abdulwahid, A., & Bakhsh, S. T. (2019). Determining factors pertaining to cloud security adoption framework in government organizations: an exploratory study. IEEE Access, 7, 136822-136835.

[94] Kaisler, S., Money, W. H., & Cohen, S. J. (2012, January). A decision framework for cloud computing. In 2012 45th Hawaii International Conference on System Sciences (pp. 1553-1562). IEEE.

προσδιοριστούν οι επιχειρηματικοί στόχοι που θα επιτευχθούν όταν θα γίνει η μετάβαση στο υπολογιστικό νέφος. Για αυτό το σκοπό θα πρέπει να γίνει μια ανάλυση κόστους-οφέλους που θα επιτρέψει την κατανόηση του σκοπού της επιχείρησης για μετάβαση στο υπολογιστικό νέφος και πώς αυτό ευθυγραμμίζεται με τη γενικότερη στρατηγική ανάπτυξης της επιχείρησης. Θα πρέπει επίσης να αξιολογηθεί εάν οι τεχνολογίες που υποστηρίζονται από το υπολογιστικό νέφος είναι συμβατές με τα υπάρχοντα συστήματα και τις εφαρμογές που χρησιμοποιεί ήδη η επιχείρηση. Εκτός από την εξέταση των κύριων παρόχων υπηρεσιών υπολογιστικού νέφους, οι υπεύθυνοι του Τμήματος πληροφορικής θα πρέπει να συλλέξουν δεδομένα σχετικά με τις προκλήσεις και τις επιτυχίες των εταιρειών του κλάδου τους που έχουν ήδη υιοθετήσει υπηρεσίες υπολογιστικού νέφους.

7.4.2 Σχεδιασμός

Μόλις γίνει η σχετική έρευνα αγοράς, θα πρέπει να σχεδιαστεί η στρατηγική που θα ακολουθηθεί. Οι υπεύθυνοι πληροφορικής θα πρέπει να επιλέξουν πλατφόρμες και υπηρεσίες που είναι γνωστές στον κλάδο τους. Κατά την επιλογή του παρόχου θα πρέπει να δοθεί έμφαση σε χαρακτηριστικά όπως η εμπειρία, η τεχνική επάρκεια, η ηγετική θέση στην αγορά, η φήμη, η ικανοποίηση πελατών και οι λύσεις που μπορεί να δώσει για το χειρισμό των ενημερώσεων. Θα πρέπει επίσης να αποφασίσει η επιχείρηση μεταξύ δημόσιου, ιδιωτικού ή υβριδικού υπολογιστικού νέφους.

7.4.3 Υιοθέτηση

Κατά τη φάση της υιοθέτησης, οι υπεύθυνοι πληροφορικής θα πρέπει να αναπτύξουν στρατηγικές μετριασμού του κινδύνου. Θα πρέπει επίσης να έχουν μια εξειδικευμένη κατανόηση των διακομιστών, του λογισμικού και των δεδομένων τους για τη μελλοντική επανάληψη και επεκτασιμότητα της στρατηγικής τους.

7.4.4 Βελτιστοποίηση

Οι συμμετέχοντες σε αυτή τη διαδικασία θα πρέπει να συζητήσουν τα διδάγματα που έχουν αντλήσει από τη στρατηγική τους σχετικά με τη χρήση υπηρεσιών υπολογιστικού νέφους, και να δημιουργήσουν νέες και βελτιωμένες λύσεις για περαιτέρω σχετικές διαδικασίες.

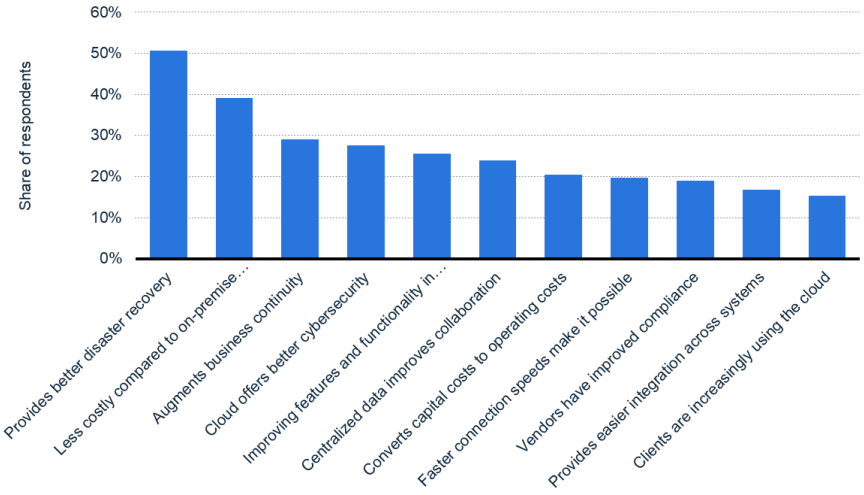
7.5 Χρήση υπηρεσιών υπολογιστικού νέφους από δικηγόρους/δικηγορικές εταιρίες

Οι επαγγελματίες του κλάδου της Νομικής λόγω των ιδιαίτερων χαρακτηριστικών των πληροφοριών που διαχειρίζονται θα πρέπει να είναι ιδιαίτερα προσεκτικοί κατά τη χρήση υπηρεσιών υπολογιστικού νέφους. Κατά την αναζήτηση παρόχων θα πρέπει να εξετάσουν ζητήματα που αφορούν την πρόσβαση στα δεδομένα, συμβατικές διατάξεις για αποκάλυψη εμπιστευτικών πληροφοριών συμπεριλαμβανομένων των δεδομένων πελατών σε τρίτα μέρη, αλλά και της περίπτωσης όπου λόγω δικαστικών αποφάσεων μπορεί να απαιτείται η μη καταστροφή των δεδομένων που διατηρούνται στο υπολογιστικό νέφος του παρόχου ή σε εφεδρικά μέσα[95]. Βέβαια τα παραπάνω θα πρέπει να συσχετιστούν και με τα πιθανά οφέλη που παρέχουν οι υπηρεσίες υπολογιστικού νέφους τα οποία αναλύθηκαν παραπάνω. Μάλιστα οι επαγγελματίες του κλάδου θα πρέπει να έχουν υπόψη ότι καθώς οι καταναλωτές, ιδίως λόγω και της πανδημίας, έχουν ήδη συνηθίσει να απολαμβάνουν τις διαδικτυακές υπηρεσίες για πολλές άλλες πτυχές της ζωής τους, η παροχή μιας διαδικτυακής υπηρεσίας με επίκεντρο τον πελάτη και σε θέματα νομικών υπηρεσιών θα μπορούσε να αυξήσει το πελατολόγιο τους.

Τον Απρίλιο του 2018 η Aderant πραγματοποίησε έρευνα[96] σχετικά με τους παράγοντες που οδήγησαν δικηγορικά γραφεία παγκοσμίως στην υιοθέτηση υπηρεσιών υπολογιστικού νέφους. Σύμφωνα με την έρευνα, το 50,5% των ερωτηθέντων δήλωσε ότι υιοθετεί λύσεις που βασίζονται στο υπολογιστικό νέφος, καθώς παρέχουν καλύτερη ανάκτηση δεδομένων σε περίπτωση καταστροφών. Άλλοι παράγοντες που αναφέρθηκαν είναι ότι έχει μικρότερο κόστος σε σχέση με άλλες λύσεις, συμβάλλει στη συνέχεια της επιχείρησης, παρέχει καλύτερη κυβερνοασφάλεια, βελτίωση χαρακτηριστικών και λειτουργικότητας σε προϊόντα υπολογιστικού νέφους, η συγκέντρωση των δεδομένων βελτιώνει τη συνεργασία, μετατροπή κεφαλαιουχικού κόστους σε λειτουργικό κόστος, ταχύτερη σύνδεση, οι πάροχοι έχουν βελτιώσει τη

[95] McCauley, J. M. (2011). Cloud Computing–A Silver Lining or Ethical Thunderstorm for Lawyers. Virginia Lawyer, 59, 49-54.
[96] 2018 Aderant Business of Law and Legal Technology Survey

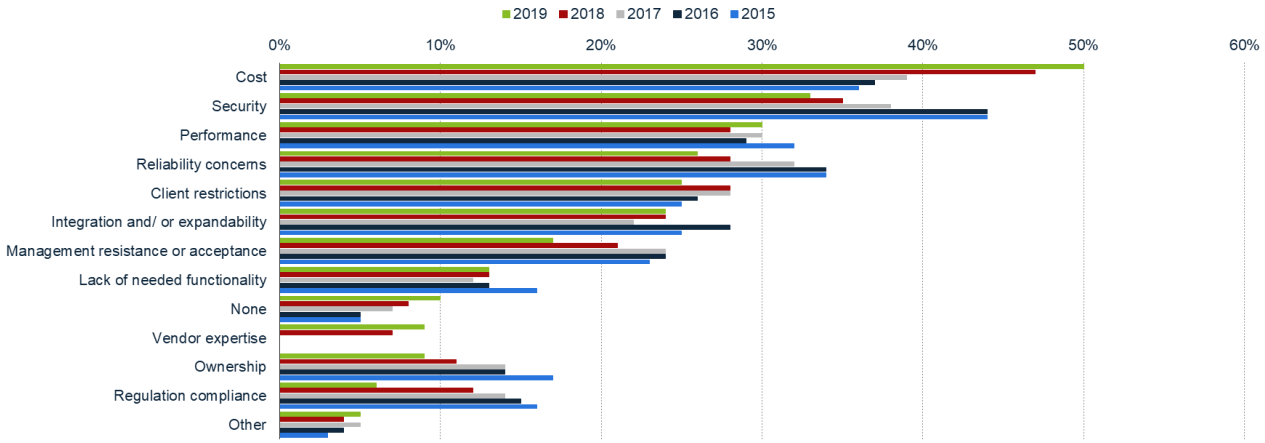
συμμόρφωσή τους στα κανονιστικά πλαίσια, ευκολότερη ενοποίηση μεταξύ συστημάτων, οι πελάτες όλο και περισσότερο χρησιμοποιούν εφαρμογές υπολογιστικού νέφους.



Διάγραμμα 4: Παράγοντες που οδήγησαν στην υιοθέτηση υπηρεσιών υπολογιστικού νέφους από δικηγορικά γραφεία παγκοσμίως το 2018

Πηγή: 2018 Aderant Business of Law and Legal Technology Survey

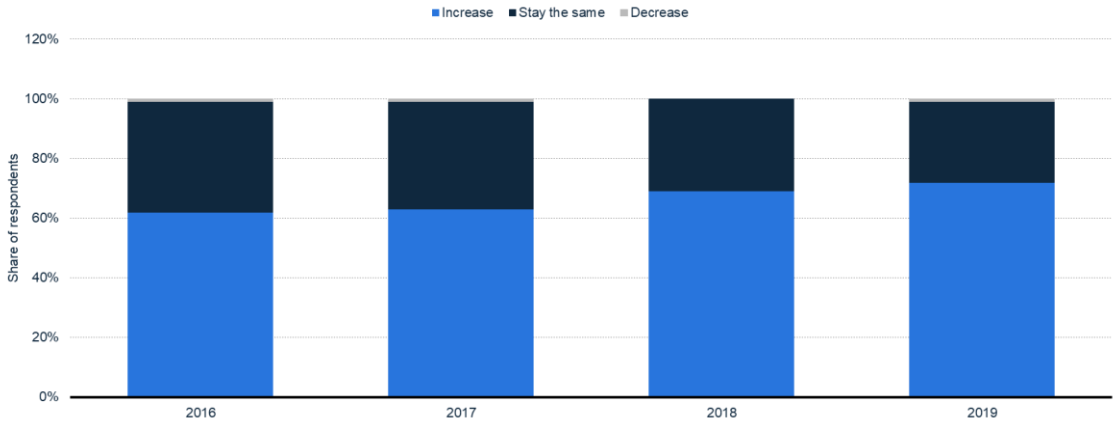
Στο ILTA[97] 2019 Technology Survey παρουσιάζονται τα εμπόδια για τις δικηγορικές εταιρείες παγκοσμίως να μεταφέρουν τις εργασίες τους στο υπολογιστικό σύννεφο μεταξύ 2015 και 2019. Σύμφωνα με την έρευνα, το 50% των δικηγορικών γραφείων ανέφεραν το κόστος ως εμπόδιο για την υιοθέτηση λύσεων υπολογιστικού νέφους. Ακολουθούν θέματα ασφάλειας, αποτελεσματικότητας, αξιοπιστίας, περιορισμών των πελατών, διασύνδεσης, συμμόρφωσης κ.α.



[97] International Legal Technology Association

Διάγραμμα 5: Παράγοντες που εμπόδισαν στην υιοθέτηση υπηρεσιών υπολογιστικού νέφους από δικηγορικά γραφεία παγκοσμίως την περίοδο 2015 – 2019
Πηγή: ILTA 2019 Technology Survey

Ωστόσο, θα πρέπει να αναφερθεί ότι στην ίδια μελέτη το 72% των δικηγορικών γραφείων δήλωσαν ότι θα αυξήσουν τη χρήση λύσεων που βασίζονται σε υπολογιστικό νέφος κατά τη διάρκεια του επόμενου έτους.



Διάγραμμα 6: Μεταβολή κατά τη διάρκεια του επόμενου έτους στη χρήση τεχνολογίας που βασίζεται στο υπολογιστικό νέφος από δικηγορικά γραφεία σε όλο τον κόσμο το 2019
Πηγή: ILTA 2019 Technology Survey

8 Κοινωνικές και πολιτικές εξελίξεις στην υπολογιστική νέφους

Είναι μάλιστα τόσο μεγάλο το ενδιαφέρον για το υπολογιστικό νέφος που τον Οκτώβριο του 2020 είκοσι πέντε χώρες της Ε.Ε., ανάμεσα στις οποίες και η Ελλάδα, και η Κομισιόν προανήγγειλαν τη συγκρότηση «Συμμαχίας για τα βιομηχανικά δεδομένα» μέχρι το τέλος του 20200, με προφανή στόχο να βάλουν φρένο στη μονοπώληση του πεδίου από τις αμερικανικές ψηφιακές πολυεθνικές και συνυπέγραψαν διακήρυξη υπέρ μιας «ομοσπονδίας (υπολογιστικών) νεφών» στην Ένωση και το γεγονός αυτό χαιρέτισαν η Ευρωπαϊκή Επιτροπή και η τότε γερμανική προεδρία της Ε.Ε.

Τον Ιούλιο του 2021 η Ευρωπαϊκή Επιτροπή εγκαινιάζει δύο νέες βιομηχανικές συμμαχίες με στόχο την ψηφιακή κυριαρχία της Ευρώπης: α) τη συμμαχία για τους επεξεργαστές και τις τεχνολογίες ημιαγωγών, και β)την ευρωπαϊκή συμμαχία για τα βιομηχανικά δεδομένα, την υπολογιστική παρυφών και το υπολογιστικό νέφος.

Η κ. Μαργκρέτε Βεστάγκερ, εκτελεστική αντιπρόεδρος για μια Ευρώπη Έτοιμη για την Ψηφιακή Εποχή, δήλωσε σχετικά: «Οι τεχνολογίες υπολογιστικού νέφους και υπολογιστικής παρυφών παρουσιάζουν τεράστιες οικονομικές δυνατότητες για τους πολίτες, τις επιχειρήσεις και τις δημόσιες διοικήσεις, για παράδειγμα όσον αφορά την αύξηση της ανταγωνιστικότητας και την κάλυψη συγκεκριμένων αναγκών της βιομηχανίας. Τα μικροτσίπ βρίσκονται στον πυρήνα κάθε συσκευής που χρησιμοποιούμε σήμερα. Από τα κινητά μας τηλέφωνα έως τα διαβατήριά μας, τα μικρά αυτά εξαρτήματα προσφέρουν πληθώρα ευκαιριών για τεχνολογικές εξελίξεις. Ως εκ τούτου, η στήριξη της καινοτομίας στους εν λόγω κρίσιμους τομείς είναι ζωτικής σημασίας και μπορεί να βοηθήσει την Ευρώπη να προοδεύσει μαζί με εταίρους που συμμερίζονται τις ίδιες απόψεις».

Όπως τονίζεται στην Ευρωπαϊκή Στρατηγική για τα Δεδομένα, ο όγκος των δεδομένων που παράγονται αυξάνεται σημαντικά και ένα σημαντικό ποσοστό δεδομένων αναμένεται να υποβληθεί σε επεξεργασία στο «όριο» (“edge”) (80% έως το 2025, από μόνο 20% σήμερα), πιο κοντά στους χρήστες και όπου παράγονται τα δεδομένα. Αυτή η μετατόπιση αντιπροσωπεύει μια σημαντική ευκαιρία για την ΕΕ να ενισχύσει τις δικές της ικανότητες “cloud” και “edge”, και συνεπώς τις τεχνολογικές δυνατότητές της για κυριαρχία.

Σύμφωνα με το από 19 Ιουλίου 2021 Δελτίο Τύπου της Ευρωπαϊκής Επιτροπής, Βρυξέλλες[98] :

«….Η ευρωπαϊκή συμμαχία για τα βιομηχανικά δεδομένα, τις παρυφές και το υπολογιστικό νέφος θα προωθήσει την εμφάνιση ανατρεπτικών τεχνολογιών στον εν λόγω κλάδο, που θα είναι υψηλής ασφάλειας, αποδοτικές ως προς την ενέργεια και τη χρήση των πόρων και πλήρως διαλειτουργικές, ενώ θα ενισχύσει την εμπιστοσύνη των

[98] Δελτίο Τύπου Ευρωπαϊκής Επιτροπής, 19 Ιουλίου 2021 Βρυξέλλες (https://ec.europa.eu/commission/presscorner/detail/el/IP_21_3733).

χρηστών του υπολογιστικού νέφους σε όλους τους τομείς. Η συμμαχία θα εξυπηρετεί τις ειδικές ανάγκες των πολιτών, των επιχειρήσεων και του δημόσιου τομέα της ΕΕ (μεταξύ άλλων για σκοπούς στρατιωτικούς και ασφάλειας) σχετικά με την επεξεργασία εξαιρετικά ευαίσθητων δεδομένων, ενώ παράλληλα θα ενισχύσει την ανταγωνιστικότητα της βιομηχανίας της ΕΕ στον τομέα των τεχνολογιών υπολογιστικού νέφους και υπολογιστικής παρυφών. Καθ' όλη τη διάρκεια ζωής της συμμαχίας αυτής, το έργο της θα τηρεί τις ακόλουθες βασικές αρχές και κανόνες:

-υψηλότερα πρότυπα όσον αφορά τη διαλειτουργικότητα και τη φορητότητα/ αναστρεψιμότητα, τον ανοιχτό χαρακτήρα και τη διαφάνεια·
-υψηλότερα πρότυπα όσον αφορά την προστασία των δεδομένων, την κυβερνοασφάλεια και την κυριαρχία των δεδομένων·
-κορυφαία ενεργειακή απόδοση και βιωσιμότητα·
-συμμόρφωση με τις ευρωπαϊκές βέλτιστες πρακτικές υπολογιστικού νέφους, μεταξύ άλλων μέσω της τήρησης των σχετικών προτύπων, κωδίκων δεοντολογίας και συστημάτων πιστοποίησης».

Στις 9 Δεκεμβρίου, η Ευρωπαϊκή Επιτροπή ανακοίνωσε ότι ζήτησε επίσημα από τον Οργανισμό της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια (European Union Agency for Cybersecurity-ENISA) να προετοιμάσει ένα υποψήφιο σύστημα πιστοποίησης κυβερνοασφάλειας για το cloud (European Union Cybersecurity Certification Scheme on Cloud Services-EUCS on Cloud Services), λαμβάνοντας υπόψη τις προηγούμενες εισροές μας από το CSPCERT (European Cloud Provider Certification) που είναι μια ιδιωτική και δημόσια Ομάδα Εργασίας ενδιαφερομένων. Ο ENISA αποδέχτηκε το αίτημα, θα αναπτύξει ένα σχέδιο για υποδομές και υπηρεσίες cloud και θα υποβάλει την πρότασή του στην Ευρωπαϊκή Επιτροπή για επίσημη έγκριση. Η εκπόνηση ενός τέτοιου συστήματος πιστοποίησης θα ενισχύσει περαιτέρω την ασφάλεια και την εμπιστοσύνη στις υπηρεσίες cloud στην Ευρώπη.

Έτσι ο ENISA ξεκίνησε στις 22 Δεκεμβρίου 2020 τη δημόσια διαβούλευση, η οποία ολοκληρώθηκε στις 7 Φεβρουαρίου του 2021 σχετικά με το προσχέδιο του υποψηφίου συστήματος πιστοποίησης κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης στις Υπηρεσίες Cloud (EUCS). Ο Εκτελεστικός Διευθυντής του ENISA, Juhan Lepassaar, δήλωσε : « Οι υπηρεσίες cloud διαδραματίζουν αυξανόμενο ρόλο στη ζωή των

ευρωπαίων πολιτών και επιχειρήσεων που βρίσκονται υπό lockdown και η ασφάλειά τους είναι απαραίτητη για τη λειτουργία της ψηφιακής ενιαίας αγοράς. Μια ενιαία ευρωπαϊκή πιστοποίηση cloud είναι κρίσιμη για τη διευκόλυνση της ελεύθερης ροής δεδομένων σε όλη την Ευρώπη και είναι σημαντικός παράγοντας για την προώθηση της καινοτομίας και της ανταγωνιστικότητας στην Ευρώπη»[99].

Το προσχέδιο του υποψηφίου συστήματος πιστοποίησης κυβερνοασφάλειας της Ευρωπαϊκής Ένωσης στις Υπηρεσίες Cloud (EUCS) έχει τα εξής χαρακτηριστικά (σύμφωνα με το επίσημο δελτίο τύπου του ENISA)[87]:

- Είναι ένα εθελοντικό σύστημα.
- Τα πιστοποιητικά του συστήματος θα ισχύουν σε όλα τα κράτη μέλη της ΕΕ.
- Ισχύει για όλα τα είδη υπηρεσιών cloud – από υποδομές έως εφαρμογές.
- Ενισχύει την εμπιστοσύνη στις υπηρεσίες cloud ορίζοντας ένα σύνολο αναφοράς απαιτήσεων ασφαλείας.
- Καλύπτει τρία επίπεδα διασφάλισης: «Βασικό», «Ουσιαστικό» και «Υψηλό». Προτείνει μια νέα προσέγγιση εμπνευσμένη από τα υπάρχοντα εθνικά συστήματα και τα διεθνή πρότυπα·
- Καθορίζει μια διαδρομή μετάβασης από τα εθνικά συστήματα στην ΕΕ·
- Χορηγεί τριετή πιστοποίηση που μπορεί να ανανεωθεί·
- Περιλαμβάνει απαιτήσεις διαφάνειας, όπως η τοποθεσία επεξεργασίας και αποθήκευσης δεδομένων.

[99] Δελτίο Τύπου ENISA της 22ας Δεκεμβρίου 2020, για το «Πρόγραμμα Πιστοποίησης Cloud», https://www-enisa-europa-eu.translate.goog/news/enisa-news/cloud-certification-scheme?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc

9 Συμπεράσματα

Στην παρούσα διπλωματική εξετάστηκε η υπολογιστική νέφους, ως τεχνολογία αιχμής και συγκέντρωσης παγκόσμιου ενδιαφέροντος, υπό το πρίσμα των νομικών κυρίως και οικονομικών προεκτάσεων της λειτουργίας και εφαρμογής της, σε συνδυασμό με τις κοινωνικές και πολιτικές εξελίξεις που επιφέρει. Η υπολογιστική νέφους, όπως εμφανίζεται και εφαρμόζεται μέσα από τις τεχνικές εκδοχές και τα μοντέλα ανάπτυξής της, στηρίζεται στη λειτουργία του διαδικτύου. Αυτό την καθιστά «ατοπική» και πολυεπίπεδη. Απεριόριστος αριθμός χρηστών έχει πρόσβαση στις υπηρεσίες νέφους. Ζητούμενο είναι να υπάρξει μια σταθερή περαιτέρω αύξηση της ζήτησης των υπηρεσιών αυτών με την παράλληλη, διαρκή οικοδόμηση και ενίσχυση ενός κλίματος εμπιστοσύνης, ασφάλειας και αξιοπιστίας μεταξύ παρόχων και πελατών. Στην κατεύθυνση αυτή εξετάστηκαν και συγκεντρώθηκαν όλα εκείνα τα νομικά μέσα, και κυρίως τα πολύ πρόσφατα και επικαιροποιημένα, που επιστρατεύει η Ευρωπαϊκή Ένωση τόσο για τη ρύθμιση των πολλαπλών νομικών θεμάτων από την παροχή και λήψη υπηρεσιών νέφους εντός του ΕΟΧ όσο και σε σχέση με τρίτες χώρες όπως οι ΗΠΑ. Ανάμεσα σε αυτά κυρίαρχο ρόλο διαδραματίζει ο ΓΚΠΔ για την προστασία των προσωπικών δεδομένων, ως ένας Κανονισμός συνεκτικότητας. Με γνώμονα αυτόν, οριοθετούνται τα δικαιώματα και υποχρεώσεις των μερών ως προς την επεξεργασία των προσωπικών δεδομένων, αφού προηγουμένως έχουν διακριθεί στην παρούσα οι ρόλοι υπεύθυνος επεξεργασίας και εκτελών την επεξεργασία και έχουν αποδοθεί στους χρήστες και στους παρόχους ανάλογα με τον τρόπο που ενεργούν κάθε φορά μέσα στην αλυσίδα των υπηρεσιών νέφους.

Στην προσπάθεια συμμόρφωσης με την Οδηγία 95/46/ΕΚ και μετέπειτα με τον ΓΚΠΔ συνήφθησαν σταδιακά και εφαρμόστηκαν οι διεθνείς συμφωνίες του Ασφαλούς Λιμένα και της Ασπίδας προστασίας με τις ΗΠΑ, οι οποίες συμφωνίες ακυρώθηκαν με δύο πολύκροτες και κομβικές αποφάσεις του ΔΕΕ, όπως σχολιάστηκαν στην παρούσα, λόγω παραβιάσεων που διαπιστώθηκαν στην προστασία των προσωπικών δεδομένων και ανέδειξαν την έλλειψη επαρκούς και ικανοποιητικού επιπέδου ασφάλειας και εμπιστευτικότητας. Το «κενό που δημιουργήθηκε κλήθηκαν να αναπληρώσουν σε σημαντικό βαθμό οι τυποποιημένες συμβατικές ρήτρες (SCC) που καθιέρωσε η Ε.Ε. και μάλιστα οι πιο πρόσφατε,ς που τέθηκαν σε ισχύ στις 27-6-2021

και καταργούν και τροποποιούν τις προηγούμενες μετά από ένα μεταβατικό υπό προϋποθέσεις χρονικό διάστημα. Επιστρατεύονται ακόμη Δεσμευτικοί Εταιρικοί Κανόνες, Κώδικες Δεοντολογίας και πρότυπα ISO. Ξεχωρίζουν οι EU CLOUD CoC και Code of Conduct of CISPE κώδικες δεοντολογίας, που εγκρίθηκαν από τη Βελγική και Γαλλική Εποπτική Αρχή αντίστοιχα, σύμφωνα με τις θετικές γνώμες του ΕΣΠΔ, αλλά και το ISO/IEC 27018:2019 όπως αναθεώρησε και τροποποίησε το προϋφιστάμενο ISO/IEC 27018:2014.

Τα παραπάνω επικαιροποιημένα νομικά μέσα έχουν πολλά να εισφέρουν αν εφαρμοστούν και ενσωματωθούν στις συμβάσεις υπολογιστικού νέφους που καταρτίζουν οι πάροχοι υπηρεσιών νέφους με τους πελάτες-χρήστες, και κυρίως θα μπορούσαν να χτίσουν ένα ισχυρό πλέγμα εμπιστοσύνης και αξιοπιστίας. Περαιτέρω ο νομικός χαρακτηρισμός των συμβάσεων αυτών ερευνάται για να εφαρμοστούν οι αντίστοιχοι κανόνες δικαίου, αλλά και για να δοθεί στη συνέχεια απάντηση στο θέμα της διεθνούς δικαιοδοσίας ως προς την επίλυση διαφορών που προκύπτουν από τη λειτουργία των συμβάσεων υπολογιστικού νέφους και των έννομων σχέσεων που αναπτύσσονται μεταξύ των μερών. Αν προκριθεί ο χαρακτηρισμός των συμβάσεων υπολογιστικού νέφους ως συμβάσεων παροχής υπηρεσιών θα υπαχθούν στη δικαιοδοσία του άρθρου 7 παρ. 1 εδάφιο β΄ του Κανονισμού Βρυξελλών Ια. Σύμφωνα με αυτό, η δικαιοδοσία τοποθετείται στον τόπο εκπλήρωσης της παροχής. Για να εντοπιστεί ο τόπος εκπλήρωσης της παροχής των υπηρεσιών, θα εξεταστεί αρχικά αν με κάποιο όρο της ίδιας της σύμβασης έχει προσδιοριστεί ρητά ο τόπος εκπλήρωσης της παροχής των υπηρεσιών ή αν περιέχονται ισχυρά στοιχεία από τα οποία συνάγεται. Αν δεν προκύψει ο τόπος εκπλήρωσης της παροχής των υπηρεσιών από τη σύμβαση, τότε πρέπει εν αμφιβολία να αναζητηθεί στον τόπο εγκατάστασης του παρέχοντος τις υπηρεσίες. Στις περιπτώσεις που μοιράζεται η δραστηριότητά του μεταξύ περισσότερων κρατών μελών, θα πρέπει να εντοπίζεται ως τόπος εγκατάστασης του παρόχου ο τόπος των κύριων δραστηριοτήτων οργάνωσης και εκτέλεσης των εν λόγω υπηρεσιών.

Ως προς τις οικονομικές διαστάσεις της υπολογιστικής νέφους διαπιστώνεται μια σταθερή, έντονα αυξητική τάση στη ζήτηση των υπηρεσιών υπολογιστικού νέφους και ταυτόχρονα μια μεγάλη άνοδος της οικονομικής αξίας της παγκόσμιας αγοράς εφαρμογών υπολογιστικού νέφους και παροχής υπηρεσιών υπολογιστικού νέφους.

Υπάρχουν πολλά οφέλη από την υιοθέτηση και χρήση των υπηρεσιών «νέφους», αλλά και σημαντικές προκλήσεις, η διαχείριση των οποίων καθιστά απαραίτητο το να απαντηθούν πρώτα συγκεκριμένα ερωτήματα από τις επιχειρήσεις πριν την μετάβαση στο υπολογιστικό νέφος και να ακολουθηθούν κάποια στάδια στη λήψη αποφάσεων.

Τέλος, έγινε μνεία των πρωτοβουλιών, των ενεργειών και των συμμαχιών που διαμορφώνει η ΕΕ, ως απόδειξη του έντονου ενδιαφέροντος για το υπολογιστικό νέφος και της καίριας θέσης που αυτό κατέχει στην ψηφιακή αγορά.

10 Βιβλιογραφία - Αρθρογραφία

10.1 Ελληνόγλωσση

- Αλεξανδροπούλου – Αιγυπτιάδου Ε., 2016, Προσωπικά Δεδομένα, εκδόσεις Νομική Βιβλιοθήκη.
- Ahmed S., 2014, Υπολογιστικό Νέφος (cloud computing): Θέματα σύναψης συμβάσεων και συμμόρφωσης για νομικούς συμβούλους, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ , 6/2014.
- Κουσουνή-Πανταζοπούλου Α., 2012, Νομικές διαστάσεις του Cloud computing, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ, 2/2012.
- Μήτρου Λ., 2015, Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος, Νομική Βιβλιοθήκη - Περιοδικά - ΔΙΚΑΙΟ ΜΕΣΩΝ ΕΝΗΜΕΡΩΣΗΣ & ΕΠΙΚΟΙΝΩΝΙΑΣ, 4/2015.
- Μήτρου Λ., 2017, Ο γενικός κανονισμός προστασίας προσωπικών δεδομένων¸ νέο δίκαιο, νέες υποχρεώσεις, νέα δικαιώματα, εκδόσεις Σάκκουλα.
- Ρεβολίδης Ι., 2020, Διεθνής Δικαιοδοσία και διαδίκτυο, ο νομικός χαρακτηρισμός των συμβάσεων «υπολογιστικού νέφους», εκδόσεις Σάκκουλα.
- Σμυρνάκη Ε., 2016, Υπολογιστικό Νέφος (Cloud) και Προσωπικά Δεδομένα - Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016, Pro Justitia, Τόμος 2/2016.

10.2 Ξενόγλωσση

- Alassafi, M. O., AlGhamdi, R., Alshdadi, A., Al Abdulwahid, A., & Bakhsh, S. T., 2019, Determining factors pertaining to cloud security adoption framework in government organizations: an exploratory study. IEEE Access, 7, pp.136822-136835.
- Kaisler, S., Money, W. H., & Cohen, S. J., 2012, A decision framework for cloud computing. In IEEE 2012 45th Hawaii International Conference on System Sciences, pp. 1553-1562.
- Kumar, P. R., Raj, P. H., & Jelciana, P., 2018, Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, pp.691-697.
- McCauley, J. M., 2011, Cloud Computing–A Silver Lining or Ethical Thunderstorm for Lawyers. Virginia Lawyer, 59, pp.49-54.

- Petroli M., Alderton S. & Markiles, LLP, 2021, New Standard Contractual Clauses under the GDPR, National Law Review, Volume XI, Number 221.

10.3 Νομοθεσία – Νομολογία

- Άρθρο 3 παρ. 1 και 2 ΓΚΠΔ
- Άρθρο 4 παρ. 7 και 8 ΓΚΠΔ
- Άρθρο 5 ΓΚΠΔ
- Άρθρο 17 ΓΚΠΔ
- Άρθρο 20 ΓΚΠΔ
- Άρθρο 27 παρ. 2 ΓΚΠΔ
- Άρθρο 28 ΓΚΠΔ
- Άρθρο 32 ΓΚΠΔ
- Άρθρο 33 ΓΚΠΔ
- Άρθρο 40 ΓΚΠΔ
- Άρθρο 41 ΓΚΠΔ
- Άρθρο 45 ΓΚΠΔ
- Άρθρο 46 ΓΚΠΔ
- Άρθρο 57 παρ. στοιχείο ιθ ΓΚΠΔ
- Άρθρο 58 παρ. 3 στοιχείο ι ΓΚΠΔ
- Άρθρο 63 ΓΚΠΔ
- Άρθρο 64 ΓΚΠΔ
- Άρθρο 65 ΓΚΠΔ
- Άρθρο 68 ΓΚΠΔ
- Αιτιολογική σκέψη 23 του Κανονισμού (ΕΕ) 2016/679
- Αιτιολογική σκέψη 24 του Κανονισμού (ΕΕ) 2016/679
- Αιτιολογική σκέψη 30 του κανονισμού (ΕΕ) 2016/679
- Αιτιολογική σκέψη 109 του κανονισμού (ΕΕ) 2016/679
- Κανονισμός Βρυξελλών Ια. (1215/2012), άρθρο 7 παρ. 1 στοιχείο β΄.
- Γνώμη 1/2010 Ομάδας ΄Αρθρου 29 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf
- Γνώμη 5/2012 Ομάδας ΄Αρθρου 29 σχετικά με τη νεφοϋπολογιστική, σελ.12-14,

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation /files/2012 /wp196_en. pdf

- Γνώμη 16/2021 του ΕΣΠΔ της 19ης Μαΐου 2021, https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-162021-draft-decision-belgiansupervisory_el
- Γνώμη 17/2021 του ΕΣΠΔ της 19ης Μαΐου 2021.
- ΔΕΕ υπόθεση C-19/09 (Wood Floor Solutions κατά Silva Trade SA).
- ΔΕΕ C-469/12 (υπόθεση Krejci Lager & Umshlagbetriebs GmbH κατά Olbrich Transport und Logistik GmbH)
- ΔΕΕ της 6ης Οκτωβρίου 2015 στην υπόθεση C-362/2014, «Maximilian Schrems κατά Data Protection Commissioner», EU:C:2015:650 https://curia.europa.eu/juris/document/document.jsf;jsessionid=4D2338BD91AC1AE7CD32F9F62E983FD8?text&docid=169195&pageIndex=0&doclang=EL&mode=lst&dir&occ=first&part=1&cid=744279
- ΔΕΕ της 16ης Ιουλίου 2020 στην υπόθεση C-311/18 (Schrems II), «Data Protection Commissioner κατά Facebook Ireland Limited και Maximillian Schrems», EU:C:2020:559, https://curia.europa.eu/juris/liste.jsf?num=C-311/18, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A62018CJ0311
- Έκθεση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και Συμβούλιο «σχετικά με την τρίτη ετήσια επανεξέταση της λειτουργίας της ασπίδας προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ», {SWD(2019) 390 final}, Βρυξέλλες, 23.10.2019, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52019DC0495&from=ES
- Εκτελεστική απόφαση (ΕΕ) 2016/1250 της Επιτροπής, της 12ης Ιουλίου 2016, βάσει της Οδηγίας 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την επάρκεια της προστασίας που παρέχεται από την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ (ΕΕ L 207 της 1.8.2016, σ. 1).
- Εκτελεστική Απόφαση (ΕΕ) 2021/914 της Επιτροπής, Τμήμα ΙΙΙ των ρητρών, «Τοπική νομοθεσία και υποχρεώσεις σε περίπτωση πρόσβασης από τις δημόσιες αρχές», Ρήτρα 14 και 15, σελ. 22,23.
- Εκτελεστική Απόφαση (ΕΕ) 2021/914 της Επιτροπής, άρθρο 4,

https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32021D0914&from=EN

- Σχόλιο Ευάγγελου Βασιλακάκη στην υπόθεση ΔΕΕ υπόθεση C19/09 (Wood Floor Solutions κατά Silva Trade SA), ΕΠολΔ 2010.

10.4 Διαδικτυακές πηγές

- Ανακοίνωση της Ευρωπαϊκής Επιτροπής στο Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο, την Ευρωπαϊκή Οικονομική και Κοινωνική Επιτροπή και την Επιτροπή των Περιφερειών για την «Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους», COM(2012)529nal, http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EL:PDF
- Αρχές απορρήτου Safe Harbor, ENISA (European Union Agency for Cybersecurity),https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/safe-harbor-privacy-principles
- Δελτίο Τύπου Ευρωπαϊκής Επιτροπής, 19 Ιουλίου 2021 Βρυξέλλες (https://ec.europa.eu/commission/presscorner/detail/el/IP_21_3733).
- Δελτίο Τύπου ENISA της 22ας Δεκεμβρίου 2020, για το «Πρόγραμμα Πιστοποίησης Cloud», https://www-enisa-europa-eu.translate.goog/news/enisa-news/cloud-certification-scheme?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc
- Εγχειρίδιο σχετικά με την ευρωπαϊκή νομοθεσία για την προστασία των προσωπικών δεδομένων ,Έκδοση 2018, Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, 2019, https://www.echr.coe.int/Documents/Handbook_data_protection_ELL.pdf
- Ευρωπαϊκή Επιτροπή, Γενική Διεύθυνση Δικαιοσύνης και Καταναλωτών, Συγκριτική μελέτη για συμβάσεις υπολογιστικού νέφους : τελική έκθεση , Υπηρεσία Εκδόσεων, 2015, https://data.europa.eu/doi/10.2838/16333
- Οδηγός για την ασπίδα προστασίας της ιδιωτικής ζωής ΕΕ-ΗΠΑ στην ιστοσελίδα http://ec.europa.eu,file:///C:/Users/WORKLA~1/AppData/Local/Temp/eu-

us_privacy_shield_guide_el_D36C3768-C302-1CD0-601EBD84989282FC_47787-5.pdf

- Aderant Business of Law and Legal Technology Survey 2018, https://www.aderant.com/research/2018-business-of-law-survey/
- Apps Run The World, www.appsruntheworld.com
- https://cispe.cloud/code-of-conduct/
- https://www.cnil.fr/en/cnil-approves-first-european-code-conduct-cloud-infrastructure-service-providers-iaas
- https://www.codeofconduct.cloud/
- https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_el
- ILTA 2019 Technology Survey, https://www.iltanet.org/resources/publications/surveys/2019ts,
- www.gartner.com
- Turbonomic, www.turbonic.com
- https://www.dpa.gr/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/schrems_II
- https://www-iso-org.translate.goog/standard/61498.html?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc
- https://www-iso-org.translate.goog/news/2015/07/Ref1983.html?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc
- Mell P. (NIST), Grance T. (NIST), Ορισμός του NIST National Institute of Standards and Technology (Σεπτέμβριος 2011), https://csrc.nist.gov/publications/detail/sp/800-145/final
- K. Psannis, University of Macedonia, Greece, Lecture Cloud Computing, http://compus.uom.gr/MLI4/document/Dialeksh_02/Lect-Cloud-2017.pdf
- https://www-enisa-europa-eu.translate.goog/topics/threat-risk-management/risk-management/current-risk/laws-regulation/data-protection-privacy/safe-harbor-privacy-principles?_x_tr_sl=en&_x_tr_tl=el&_x_tr_hl=el&_x_tr_pto=sc
- https://www.dpa.gr/index.php/el/enimerwtiko/thematikes_enotites/diavivaseis_ee/simvatikes_ritres
- https://www.dpa.gr/el/foreis/kwdikes_deodologias

- https://eucoc.cloud/en/detail/news/the-eu-cloud-code-of-conduct-becomes-first-gdpr-code-of-conduct-to-receive-green-light-from-data-pro/
- https://scope-europe.eu/en/our-scope/about-us.html