ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ (ΔΠΜΣ)

«ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ»

ΤΜΗΜΑΤΟΣ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΜΑΚΕΔΟΝΙΑΣ

ΚΑΙ

ΤΜΗΜΑΤΟΣ ΝΟΜΙΚΗΣ ΔΗΜΟΚΡΙΤΕΙΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΘΡΑΚΗΣ

Master of Science in «Law and Informatics»

Διπλωματική Εργασία

"Υπηρεσίες υπολογιστικού νέφους και επεξεργασία προσωπικών δεδομένων, με έμφαση στη διενέργεια εκτίμησης αντικτύπου για την ιδιωτικότητα ".

Βιργινία Δ. Κόκκα (Α.Μ. mli17013)

Επιβλέποντες καθηγητές: κα Ευγενία Αλεξανδροπούλου – Αιγυπτιάδου

κος Παπαδημητρίου Παναγιώτης

Θεσσαλονίκη – 2018

Περιεχόμενα

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

αναλυτ.	Αναλυτικά
ΑΠ	Άρειος Πάγος
Α.Π.Δ.Π.Χ.	Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
άρ.	άρθρο
αριθμ.	Αριθμός
βλ.	βλέπε
Κανονισμός	Γενικός Κανονισμός (ΕΕ)2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία αυτών
Ε.Ε.	Ευρωπαϊκή Ένωση
ενν.	εννοείται
επ.	επόμενα
ηλ.	ηλεκτρονική
Η/Υ	ηλεκτρονικός υπολογιστής
κλπ	και λοιπά
λ.χ.	λόγου χάρη
ν.	νόμος
ν.δ.	νομοθετικό διάταγμα
ό.π.	όπως παραπάνω
παρ.	παράγραφος
π.δ.	προεδρικό διάταγμα
περ.	Περίπτωση
πρβλ.	παράβαλε
π.χ.	παραδείγματος χάριν
Σ.Ε.Ε.	Συνθήκη της Ευρωπαϊκής Ένωσης
σελ.	σελίδα
στοιχ.	στοιχείο
ΤΠ	Τεχνολογία των Πληροφοριών
Φ.Ε.Κ.	Φύλλο Εφημερίδας Κυβερνήσεως
Cloud	Υπολογιστικό Νέφος (cloud coputing)
CNIL	Γαλλική Αρχή Προστασίας Προσωπικών Δεδομένων
CSP	Cloud Service Provider / πάροχος υπηρεσιών νέφους
CSC	Cloud Service Customer / πελάτης υπηρεσιών νέφους
DPIA	Data Protection Impact Assessment
GDPR	General Data Protection Regulation
ICO	Information Commissioner' Office
SLA	Service Legal Agreement

1 Εισαγωγή

Το Υπολογιστικό Νέφος (Cloud Computing) είναι μία ραγδαίως αναπτυσσόμενη τεχνολογία, χωρίς γεωγραφικούς περιορισμούς, με τεράστια δυναμική [τέσσερα μοντέλα ανάπτυξης: δημόσιο (public), ιδιωτικό (private), κοινοτικό (community) και υβριδικό (hybrid)], η οποία ενσωματώνει μεγάλο αριθμό τεχνολογιών (λ.χ. Big Data, Internet of Things) και χρησιμοποιείται καθημερινά από πολλούς ανθρώπους, ακόμη και εν αγνοία τους. Υπηρεσίες όπως το διαδικτυακό ηλεκτρονικό ταχυδρομείο, τα κοινωνικά δίκτυα (λ.χ. Facebook, Twitter κλπ) και άλλες (λ.χ. Spotify, Dropbox, We-transfer) συχνά βασίζονται στην τεχνολογία του υπολογιστικού νέφους.

Οι εταιρίες που χρησιμοποιούν την υπολογιστική νέφους, είτε αυτές είναι πάροχοι (providers) υπηρεσιών cloud computing είτε πρόκειται για κοινωνικά δίκτυα (online social networks - OSN), συγκεντρώνουν τεράστιο όγκο πληροφοριών (big data), τις οποίες επεξεργάζονται και συσχετίζουν με το λογαριασμό εκάστου χρήστη, με τη βοήθεια διάφορων μεθόδων ανάλυσης (π.χ. social network analysis, influence analysis, structural analysis, link analysis κλπ), αλγορίθμων και άλλων εργαλείων, τις οποίες είναι δυνατόν να διαβιβάζουν, να αποθηκεύουν και επεξεργάζονται σε διάφορα μέρη του κόσμου, ακόμη και εκτός της χώρας του χρήστη και να αναθέτουν τις ως άνω ενέργειες σε τρίτους – υπεργολάβους. Πολλά είναι τα ερωτήματα που εγείρονται σχετικά με την ασφάλεια από τη χρήση του cloud computing: πώς, που και από ποιον συλλέγονται, επεξεργάζονται, διαβιβάζονται και χρησιμοποιούνται τα δεδομένα αυτά; Σε ποιον ανήκουν; Πού αποθηκεύονται; Πώς διατηρείται ο έλεγχός;

Μείζον ζήτημα και ουσιαστική πρόκληση, αποτελεί λοιπόν, η πλήρης προστασία των δεδομένων των χρηστών, και δη των ευαίσθητων, που αποθηκεύονται σε cloud και η αποτελεσματικότητα της ακολουθούμενης από τους παρόχους της υπηρεσίας cloud πολιτικής, καθώς έχουν διττή ιδιότητα κατά περίπτωση (εκτελούντες την επεξεργασία και υπεύθυνοι επεξεργασίας) ειδικά εν όψει της εφαρμογής του Κανονισμού (ΕΕ) 2016/679[1], των νέων δικαιωμάτων των υποκειμένων και των υποχρεώσεων που αυτός επιβάλλει. Όμως και ο καταναλωτής - χρήστης ενεργεί ως υπεύθυνος επεξεργασίας δεδομένων, παρόλο που δεν έχει διαπραγματευτική δύναμη να αλλάξει τους προδιατυπωμένους όρους που προτείνει ένας ισχυρός πάροχος cloud υπηρεσιών, γιατί εναπόκειται στη διακριτική του ευχέρεια και στην τελική κρίση του ίδιου ποιον πιστοποιημένο πάροχο θα επιλέξει να εμπιστευτεί. Γίνεται επομένως φανερό ότι οι “ρόλοι” εναλλάσσονται και πως αμφότεροι πρέπει να διασφαλίζουν, λαμβάνοντας τα κατάλληλα τεχνικά μέτρα για την

1 Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulation – GDPR) υπογράφηκε στις 27 Απριλίου 2016 (L 119 της 4-5-2016). Το κείμενο του Κανονισμού είναι διαθέσιμο στην ηλ. Διεύθυνση https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679

προστασία από την απώλεια, καταστροφή, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση, την ασφάλεια των δεδομένων και της επεξεργασίας τους.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων της Ευρωπαϊκής Ένωσης (EU GDPR) επηρεάζει σημαντικά τη συμμόρφωση των δεδομένων Cloud τόσο για τους Παρόχους Υπηρεσιών Cloud (Cloud Providers) όσο και για τους Καταναλωτές (Cloud Consumers). Ο GDPR υποχρεώνει τους οργανισμούς που αποθηκεύουν, συλλέγουν και εν γένει επεξεργάζονται πληροφορίες σχετικά με τους πολίτες της ΕΕ να τηρούν τα άρθρα του, ανεξαρτήτως του τόπου όπου βρίσκονται ή όπου αποθηκεύονται τα δεδομένα.

Ένα καινοτόμο μέτρο που εισάγει ο νέος Κανονισμός, πλήρως εναρμονισμένο με την ανάγκη προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (Privacy by design / Privacy by default) είναι η υποχρέωση διενέργειας εκτίμησης αντικτύπου (Data Protection Impact Assessment - DPIA). Αποτελεί μία διαρκή διαδικασία εμπέδωσης και απόδειξης συμμόρφωσης με τον Κανονισμό καθώς αποσκοπεί στον εντοπισμό των κύριων κινδύνων που ελλοχεύουν για τα δικαιώματα των υποκειμένων των προσωπικών δεδομένων και στην προκαταβολική λήψη όλων των ενδεδειγμένων μέτρων – μηχανισμών ασφαλείας, για τη διασφάλιση της ιδιωτικότητας, της ακεραιότητας και του απορρήτου, αναγκάζοντας τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία να επανεξετάζουν συστηματικά την προβλεπόμενη και προσήκουσα με τον Κανονισμό επεξεργασία, τους σχετικούς κινδύνους και τα μέτρα για τον μετριασμό αυτών.

Πόσο εφικτή είναι όμως η διενέργεια εκτίμησης αντικτύπου στο περιβάλλον του cloud computing , τι πρέπει να ληφθεί υπόψη για τη διενέργειά της και από ποιόν;

1.1 Περίληψη

Στην παρούσα διπλωματική, αφού αναλυθεί η αρχιτεκτονική, τα χαρακτηριστικά και ο τρόπος λειτουργίας του cloud computing, θα εξετασθούν τα προβλήματα που δημιουργεί η χρήση του στην ασφάλεια των προσωπικών δεδομένων και στην κατανομή των ευθυνών των εμπλεκόμενων μερών. Έπειτα, θα αναπτυχθεί το νομοθετικό πλαίσιο του Κανονισμού 2016/679 (ΕΕ) για την προστασία των προσωπικών δεδομένων, τα δικαιώματα των υποκειμένων και οι υποχρεώσεις του υπεύθυνου και εκτελούντος την επεξεργασία. Θα επιχειρηθεί ο διαχωρισμός και η κατανομή των ρόλων του υπεύθυνου επεξεργασίας και εκτελούντος την επεξεργασία σε μία σύμβαση παροχής υπηρεσιών νέφους και θα ακολουθήσει μία ανάπτυξη των προβληματισμών που θέτει η εφαρμογή του ως άνω Κανονισμού για τους παρόχους

υπηρεσιών νεφοϋπολογιστικής. Εν τέλει, θα αναλυθεί η υποχρέωση διενέργειας εκτίμησης αντικτύπου, ως ένα μέτρο επίδειξης συμμόρφωσης με το νέο νομοθετικό πλαίσιο του Κανονισμού.

2 Τι είναι το Υπολογιστικό Νέφος

2.1 Χαρακτηριστικά του Υπολογιστικού νέφους

2.1.1 Σύντομο ιστορικό και έννοια

Η ιδέα του διαμοιρασμού υπολογιστικών πόρων, που αποτελεί βασική αρχή της υπολογιστικής μέσα σε ένα "νέφος", έχει ως πρόγονό της την "κοινωφελή υπολογιστική", μία έννοια που απαντάται τον πρώτον το έτος 1961, ενώ το έτος 1969 ο Leonard Kleinrock – επιστήμονας διευθυντής του έργου ARPANET (πρόγονος του Internet), είχε δηλώσει : "*μέχρι τώρα τα δίκτυα υπολογιστών βρίσκονται σε νηπιακή ηλικία, αλλά καθώς θα μεγαλώνουν και θα γίνουν σύνθετα , πιθανώς να δούμε τη διάδοση των υπολογιστών κοινωφελούς υπηρεσίας*".

Το κοινό, χρησιμοποιούσε μορφές κοινωφελών υπηρεσιών υπολογιστικής που βασίζονταν στο Internet ήδη από τα μέσα της δεκαετίας του 1990, μέσω διαφόρων μηχανών αναζήτησης (λ.χ. Yahoo, Google), υπηρεσιών e-mail (Hotmail, Gmail) και στην πορεία ανοικτών πλατφορμών δημοσιεύσεων (MySpace, Facebook, YouTube), δηλαδή υπηρεσίες οι οποίες επισημοποίησαν τις βασικές αρχές που αποτελούν την βάση του σύγχρονου υπολογιστικού νέφους.

Ο όρος "υπολογιστικό νέφος" πρωτοεμφανίστηκε στο χώρο των επιχειρήσεων το έτος 2006, όταν η Amazon ξεκίνησε την παροχή υπηρεσιών της Elastic Compute Cloud (EC2), που επέτρεπαν σε οργανισμούς να "εκμισθώνουν" υπολογιστική δυναμικότητα και ισχύ επεξεργασίας προκειμένου να εκτελούν τις επιχειρησιακές τους εφαρμογές, ενώ την ίδια χρονική περίοδο το Google Apps ξεκίνησε επίσης να παρέχει επιχειρησιακές εφαρμογές που βασίζονταν στο πρόγραμμα πλοήγησης[2].

Έτσι καταλήξαμε σήμερα να ορίζουμε το υπολογιστικό νέφος ως ένα μοντέλο για ενεργοποίηση πανταχού παρούσας, βολικής, κατ' απαίτηση πρόσβασης στο δίκτυο από μία διαμοιρασμένη δεξαμενή διαμορφώσιμων υπολογιστικών πόρων ΤΠ (λ.χ δικτύων, εξυπηρετητών, αποθήκευσης εφαρμογών και υπηρεσιών), που μπορούν να παρέχονται και να αποδεσμεύονται γρήγορα, με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδρασης από τον πάροχο της υπηρεσίας. Αυτό το μοντέλο νέφους αποτελείται από πέντε ουσιώδη χαρακτηριστικά, τρία μοντέλα υπηρεσίας και

2 Βλ . Thoms Erl, Cloud Computing , Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 28

τέσσερα μοντέλα ανάπτυξης (επίσημος ορισμός του NIST – National Institute of Standards and Technology)[3].

Με άλλα λόγια, υπολογιστικό νέφος, είναι η αποθήκευση, η επεξεργασία και η χρήση δεδομένων από απομακρυσμένους υπολογιστές (έξω δηλαδή από τη συσκευή του χρήστη) στους οποίους εξασφαλίζεται πρόσβαση μέσω του διαδικτύου, από οπουδήποτε και οποτεδήποτε, περιορίζοντας έτσι, ακόμη και εξαλείφοντας, την ανάγκη για κατ' ελάχιστο απαιτούμενο υλικό εξοπλισμό (hardware)[4]. Το μόνο που απαιτείται είναι μία απλή σύνδεση στο Internet.

Ο χρήστης-καταναλωτής δηλαδή, συνδέει τον υπολογιστή του στην πλατφόρμα του υπολογιστικού νέφους μέσω εξειδικευμένου λογισμικού ή απλώς μέσω ενός φυλλομετρητή (browser). Στο cloud, μεγάλα κέντρα δεδομένων με εκατοντάδες εξυπηρετητές και συστήματα αποθήκευσης δεδομένων, που στην πράξη είναι σε θέση να χειριστούν σχεδόν οποιοδήποτε λογισμικό υπολογιστή (από την επεξεργασία δεδομένων μέχρι τα βιντεοπαιχνίδια που ενδέχεται να χρειαστούν οι πελάτες) εξασφαλίζουν την επεξεργαστική ισχύ. Οι υπηρεσίες άλλοτε προσφέρονται δωρεάν (π.χ. διαδικτυακό ηλεκτρονικό ταχυδρομείο) και άλλοτε επί πληρωμή.

Η έννοια της υπολογιστικής νέφους συμπληρώνεται από την τεχνολογία του Mobile Cloud Computing (MCC), η οποία μετατρέπει το κινητό τηλέφωνο σε συσκευή με πλήρεις πόρους όσον αφορά στην υπολογιστική ισχύ, στη μνήμη, στην αποθήκευση και στην ευαισθητοποίηση του περιβάλλοντος, αλλά και από την τεχνολογία του Internet of Things (IoT) μέσω της οποίας επεκτείνεται η χρήση του cloud[5].

2.1.2 Χαρακτηριστικά Νέφους[6]

Η πλειοψηφία των εφαρμογών που επεξεργάζονται προσωπικά δεδομένα αλλά και οι χρήστες ή επιχειρήσεις του ιδιωτικού και δημόσιου τομέα, χρησιμοποιούν της υπηρεσίες του cloud computing.

Προκειμένου, ένα περιβάλλον ΤΠ να αποτελέσει ένα αποδοτικό νέφος, ώστε να είναι εφικτή η απομακρυσμένη παροχή κλιμακούμενων και μετρούμενων πόρων ΤΠ[7], απαιτείται η συνύπαρξη κάποιων χαρακτηριστικών, τα βασικότερα εκ

3 Για περισσότερα βλ. στην ηλ. Δ/νση : https://www.nist.gov/sites/default/files/documents/itl/cloud/cloud-def-v15.pdf

4 Stergiou C. – Psannis K., Efficient and secure big data delivery in cloud computing, διαθέσιμο στην ηλ δ/νση : https://link.springer.com/article/10.1007%2Fs11042-017-4590-4

5 Christos Stergiou a, Kostas E. Psannis a, Secure integration of IoT and Cloud Computing, ⁎, Byung-Gyu Kimb, Brij Guptac, December 2016

6 Thoms Erl, Cloud Computing, Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 58

7 Ως πόρος ΤΠ (IT resource) ορίζεται ένα φυσικό ή εικονικό τέχνημα που σχετίζεται με την ΤΠ λ.χ. ένας εικονικός ή φυσικός εξυπηρετητής, ένα ειδικό πρόγραμμα λογισμικού , μία συσκευή δικτύου , ένας επεξεργαστής , μία μνήμη αποθήκευσης.

των οποίων και κοινά στα περισσότερα περιβάλλοντα νέφους είναι :

i) η χρησιμοποίηση κατ' απαίτηση (on-demand -self-service).Δηλαδή η δυνατότητα ενός χρήστη να αυτοεξυπηρετείται οποιασδήποτε στιγμή επιθυμεί και ανάλογα με το τι ζητάει. Ο χρήστης μπορεί να παρέχει και να ζητήσει, μονομερώς υπολογιστικές δυνατότητες και πόρους ΤΠ – αύξηση/μείωση , αυτόματα,

ii) η πανταχού παρούσα πρόσβαση (ubiquitous network access). Το χαρακτηριστικό αυτό αναφέρεται στην απεριόριστη και από οποιουδήποτε πρόσβαση μέσω δικτύου στους υπολογιστικούς πόρους /υπηρεσίες, από ετερόκλητες συσκευές (κινητά τηλέφωνα, laptops, PDAs) και πολλούς χρήστες ταυτόχρονα, οπουδήποτε και αν βρίσκονται αυτοί (οι πόροι ΤΠ).

iii) η πολλαπλή μίσθωση (και συνεκμετάλλευση πόρων- Multitenancy). Αυτή, επιτρέπει αυτόματα, σε διαφορετικούς χρήστες νέφους, να χρησιμοποιούν τον ίδιο πόρο ΤΠ (φυσικό ή εικονικό), που ανακατανέμεται ανάλογα με τη ζήτηση, ενώ ο καθένας δεν γνωρίζει ότι ο πόρος αυτός χρησιμοποιείται και από άλλους,

iv) η ελαστικότητα (elastisity), δηλαδή η αυτόματη ικανότητα ενός νέφους να χρησιμοποιεί και κατανέμει τους πόρους (λ.χ. αποθήκευση, επεξεργασία, μνήμη, δίκτυο, εύρος ζώνης, εικονικές μηχανές) δυναμικά και ελαστικά, ανάλογα με τις ανάγκες κάθε πελάτη, σε συνθήκες χρόνου εκτέλεσης (λ.χ. αυξημένη ζήτηση το Σαββατοκύριακα) , ώστε να φαίνονται στον χρήστη απεριόριστοι.

v) η μετρούμενη χρησιμοποίηση (measured usage). Το χαρακτηριστικό αυτό, που συνδέεται με την χρήση κατ' απαίτηση, αφορά στη δυνατότητα μιας πλατφόρμας νέφους, να παρακολουθεί τη χρήση των πόρων της από τους χρήστες της, ώστε αφενός να μπορεί να χρεώσει τον πελάτη μόνο για τους συγκεκριμένους πόρους τους οποίους πραγματικά/ ή για το χρονικό διάστημα που χρησιμοποίησε, αφετέρου δε να παρέχεται διαφάνεια τόσο για τον πάροχο όσο και για τους χρήστες νέφους.

vi) η ανθεκτικότητα (resiliency)[8], που αφορά στη δυνατότητα ενός νέφους να αυξάνει/μειώνει αυτόματα τους πόρους ΤΠ, μέσω μιας μεταγωγής σε εφεδρικό σύστημα, έτσι ώστε, αν ένας πόρος εμφανίσει κάποιο πρόβλημα, η επεξεργασία να μετάγεται αυτόματα σε μια άλλη πλεονάζουσα υλοποίηση.

8 Ο ορισμός του NIST για το υπολογιστικό νέφος ορίζει μόνο τα 5 πρώτα χαρακτηριστικά, εξαιρώντας την ανθεκτικότητα. Ωστόσο, η ανθεκτικότητα αποτελεί πια ένα πολύ σημαντικό χαρακτηριστικό , άρρηκτα δεμένο με το συνηθισμένο μοντέλο υποστήριξης υπηρεσιών νεφών.

2.2 Πάροχοι, καταναλωτές (- χρήστες) νέφους και Συμφωνίες Επιπέδου Εξυπηρέτησης και Συμβάσεις Παροχής Νέφους

2.2.1 Πάροχοι και καταναλωτές νέφους[9]

Οι πάροχοι υπηρεσιών νέφους (cloud providers) είναι ο οργανισμός – εταιρία που παρέχει πόρους ΤΠ βασισμένους στο νέφος. Οι πάροχοι είναι υπεύθυνοι για τη διαχείριση, τη διοίκηση , τη συνεχή λειτουργία της συνολικής δομής του νέφους και καθιστούν τις υπηρεσίες του διαθέσιμες στους καταναλωτές, μέσω συμφωνιών και εγγυήσεων που διασφαλίζονται από Συμβάσεις Παροχής Υπηρεσιών (Service Level Agreement- SLAs, που περιγράφονται στη συνέχεια). Συνήθως, διαθέτουν τη δική τους υποδομή νέφους , δηλαδή τους πόρους ΤΠ που μισθώνουν στους καταναλωτές και αυτό τους καθιστά και ιδιοκτήτες νέφους[10].

Από την άλλη, ο καταναλωτής νέφους είναι το αντισυμβαλλόμενο μέρος των ως άνω συμβάσεων, δηλαδή ο οργανισμός ή ο άνθρωπος που με βάση ένα διακανονισμό με τον πάροχο του νέφους, χρησιμοποιεί κάποιους από τους πόρους ΤΠ ή τις υπηρεσίες. Είναι ο “πελάτης” - χρήστης των υπηρεσιών της νεφοϋπολογιστικής. Αυτός που καθορίζει τον τελικό σκοπό της επεξεργασίας και αποφασίζει να αναθέσει ή όχι την επεξεργασία και την εκχώρηση μέρους ή του συνόλου των δραστηριοτήτων επεξεργασίας σε εξωτερικό τρίτο οργανισμό – τον πάροχο[11].

2.2.2 Συμφωνίες Επιπέδου Εξυπηρέτησης– Service Legal Agreement (SLAs) και Συμβάσεις Παροχής νέφους– Cloud provisioning Contract.

Οι Συμφωνίες Επιπέδου Εξυπηρέτησης – Service Legal Agreement **(SLAs)**, είναι συμβάσεις που συνάπτονται μεταξύ παρόχων και καταναλωτών/ χρηστών νέφους και αποτελούν το βασικό σημείο των μεταξύ τους διαπραγματεύσεων, των όρων χρήσης, των εγγυήσεων και των δεικτών μέτρησης. Συγκεκριμένα, περιγράφουν τους όρους χρήσης της παρεχόμενης υπηρεσίας, τα χαρακτηριστικά της, την ποιότητά της, συμπεριφορές και περιορισμούς της, τον χρόνο διαθεσιμότητας, την απόδοση και την αξιοπιστία της, χαρακτηριστικά ασφαλείας αυτού κ.ά .

9 Το NIST Cloud Computing Architecture, ορίζει και άλλους πρόσθετους ρόλους λ.χ. Ελεγκτής νέφους, μεσίτης νέφους και φορέας νέφους. Για περισσότερα βλ ηλ δ/νση: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

10 Ιδιοκτήτης νέφους (cloud service owner) καλείται η οντότητα (άτομο ή οργανισμός, καταναλωτής ή πάροχος) στην οποία ανήκει νομικά μία υπηρεσία ή πόρος νέφους.

11 Βλ. Ομάδα εργασίας του άρθρου 29 σχετικά με τη νεφοϋπολογιστική, Γνώμη 05/2012 (20-6-2007), διαθέσιμη στην ηλ. Διεύθυνση http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

Μέρος των SLAs αποτελεί και η τυποποίηση των εγγυήσεων που οφείλουν να παρέχουν οι πάροχοι νέφους, οι όροι πληρωμής και ο τρόπος διαμόρφωσης των τιμών, οι κυρώσεις, οι αποζημιώσεις κ.ά. αλλά συνάμα καθορίζουν και τις προσδοκίες των καταναλωτών νέφους .

Δηλαδή, είναι συμβάσεις οι οποίες αφορούν περισσότερο στα τεχνικά γνωρίσματα και όρους της παρεχόμενης υπηρεσίας νέφους . Υπάρχουν διάφοροι δείκτες μέτρησης π.χ. της ποιότητας της υπηρεσίας, της διαθεσιμότητας της υπηρεσίας, της διάρκειας διακοπής λειτουργίας, αξιοπιστίας υπηρεσίας, της απόδοσης της υπηρεσίας, κλιμάκωσης της υπηρεσίας και μέτρησης της ανθεκτικότητας αυτής .

Έτσι, κρίνεται σημαντικό οι καταναλωτές νέφους να καταλαβαίνουν τους δείκτες μέτρησης μίας SLA, προκειμένου να διαλέξουν το “σωστό” για τις ανάγκες τους πάροχο και να επιτύχουν τους επιχειρηματικούς τους στόχους. Μόνο έτσι θα μπορέσουν να διασφαλίσουν ότι οι παρεχόμενες εγγυήσεις είναι ρεαλιστικές και αξιόπιστες.

Οι SLAs πρέπει να διακρίνονται από τις Συμβάσεις Παροχής Νέφους **(Cloud Provisioning Contract)**, που πρακτικά αποτελούν αναπόσπαστο τμήμα τους. Οι τελευταίες είναι το βασικό συμβόλαιο – νομικό έγγραφο - ανάμεσα στον καταναλωτή και τον πάροχο νέφους, που διαλαμβάνει όλους τους όρους και προϋποθέσεις της μεταξύ τους σχέσης, ορίζει δικαιώματα , υποχρεώσεις και ευθύνες για το κύριο αντικείμενο της παροχής.

Μία τυπική Σύμβαση Παροχής Νέφους, πρέπει να αποτελείται από τα εξής τμήματα:

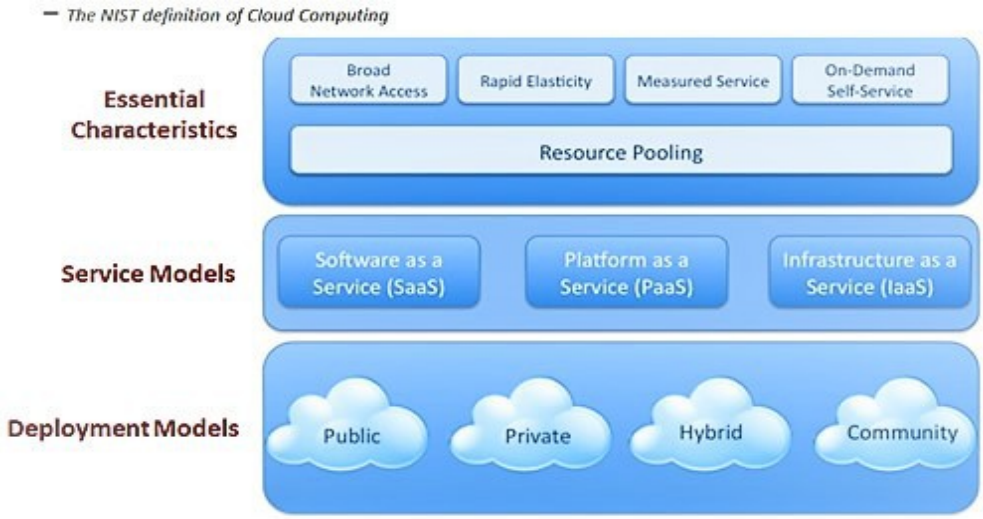
- τις τεχνικές προϋποθέσεις: εδώ καθορίζονται οι πόροι ΤΠ- υπηρεσίες που παρέχονται και οι αντίστοιχες SLA,
- τις οικονομικές προϋποθέσεις: δηλαδή οι όροι διαμόρφωσης τιμών και ο τρόπος τιμολόγησης,
- τους όρους υπηρεσιών : το βασικό τμήμα της ως άνω σύμβασης που περιέχει τους γενικούς όρους και προϋποθέσεις παροχής της υπηρεσίας, αναλύοντας την πολιτική χρησιμοποίησης της υπηρεσίας, την πολιτική ασφαλείας και ιδιωτικότητας, τις εγγυήσεις και τις ευθύνες (συμπεριλαμβανομένης και της αποζημίωσης για τη μη συμμόρφωση με τη SLA) , τα εκατέρωθεν δικαιώματα και υποχρεώσεις και τους όρους λήξης ή ανανέωσης της σύμβασης.

Ωστόσο, μέχρι σήμερα, η πρακτική έχει δείξει ότι οι εν λόγω συμβάσεις , αποτελούν μονομερείς δηλώσεις βούλησης – δέσμευσης ενός ισχυρού παρόχου Cloud, αφού πρόκειται για ηλεκτρονικής μορφής έγγραφα, οι όροι των οποίων γίνονται αποδεκτοί

από τον εκάστοτε καταναλωτή απλά με το πάτημα ενός κουμπιού στο πληκτρολόγιο του υπολογιστή του και χωρίς να είναι σε θέση να αλλάξει ίσως και κανέναν από τους προδιατυπωμένους όρους του ισχυρού αντισυμβαλλομένου του[12].

2.3 Αρχιτεκτονική του υπολογιστικού νέφους

Για να γίνει καλύτερα αντιληπτός ωστόσο ο τρόπος λειτουργίας του υπολογιστικού νέφους, ο τρόπος προσφοράς των υπηρεσιών του και οι κατηγορίες του, πρέπει να κατανοηθεί η αρχιτεκτονική του. Κατωτέρω, στην "Εικόνα 1.", αναπαριστάται οπτικά, ο ορισμός του υπολογιστικού νέφους από το NIST.



Εικόνα 1. οπτική αναπαράσταση του ορισμού του Υπολογιστικού Νέφους.

Στις παρακάτω παραγράφους, αναλύονται τα μοντέλα ανάπτυξης υπηρεσιών υπολογιστικού νέφους και τα μοντέλα επέκτασης αυτού, όπως ορίζονται από το NIST.

2.3.1 Μοντέλα ανάπτυξης υπολογιστικού νέφους

Υπάρχουν τέσσερα διαφορετικά μοντέλα ανάπτυξης του υπολογιστικού νέφους και συγκεκριμένα το δημόσιο (public), το ιδιωτικό (private), το κοινοτικό (community) και το υβριδικό (hybrid). Ο κάθε τύπος αφορά σε ένα συγκεκριμένο περιβάλλον ανάπτυξης νέφους (εφαρμογές και υπηρεσίες που παρέχει) που διακρίνεται από την ιδιοκτησία (φυσική και εγκαταστάσεις υποδομών), το μέγεθός του και την πρόσβαση . Πιο αναλυτικά :

- **Δημόσιο Νέφος**: οι εγκαταστάσεις υποδομής και οι διαθέσιμες

12 Thoms Erl, Cloud Computing , Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 404 και 39

υπηρεσίες, βασίζονται σε παγκόσμια δίκτυα κέντρων πληροφοριών και παρέχονται από τους παρόχους τους, ήτοι μεγάλους οργανισμούς- εταιρίες (λ.χ. Amazon, Google) βάσει της συμφωνίας μεταξύ παρόχου– πελάτη (SLAs). Οι πόροι ΤΠ στο εν λόγω μοντέλο παρέχονται με κάποια χρέωση ή εμπορευματοποιούνται μέσω λ.χ. διαφημίσεων. Μεγάλο πλεονέκτημά του είναι το μηδενικό κόστος επένδυσης για υποδομή, καθώς ο πάροχος του νέφους είναι υπεύθυνος για τη δημιουργία και τη συνεχή συντήρηση του νέφους και των πόρων ΤΠ αλλά κάποιες φορές και το μηδενικό κόστος για την παρεχόμενη υπηρεσία. Ωστόσο, μιας και είναι το πιο διαδεδομένο μοντέλο στο ευρύ κοινό (επομένως εύκολα προσβάσιμο και σε κακόβουλους χρήστες) εγείρονται ζητήματα εμπιστοσύνης, ασφάλειας και προστασίας των δεδομένων που διακινούνται – επεξεργάζονται σε αυτό. Η διαχείριση της ασφάλειας των δεδομένων ανατίθεται σε τρίτους και ο πελάτης – χρήστης έχει χαμηλό επίπεδο ελέγχου και εποπτείας αυτών , περιοριζόμενος συνήθως στο να αποδεχθεί απλά τους μονομερώς προδιατυπωμένους όρους του παρόχου.

- **Ιδιωτικό Νέφος** (private cloud): αυτό ανήκει σε έναν μόνο οργανισμό, όπου συνήθως βρίσκονται και οι εγκαταστάσεις υποδομής του (επιτόπια). Αυτός είναι και ο υπεύθυνος για την υποδομή και τη λειτουργία της πλατφόρμας, δηλαδή από τεχνικής σκοπιάς ο οργανισμός αυτός είναι και ο πάροχος και ο καταναλωτής. Με άλλα λόγια, το ιδιωτικό νέφος επιτρέπει στον οργανισμό να χρησιμοποιεί την τεχνολογία του νέφους, σαν έναν τρόπο κεντρικοποίησης της πρόσβασης στους πόρους ΤΠ, από διαφορετικά μέρη ή τοποθεσίες και διαφορετικά τμήματά του. Επομένως, προσφέρει μεγαλύτερο έλεγχο, εμπιστοσύνη και ασφάλεια. Ωστόσο το κόστος υποδομής του είναι μεγαλύτερο από το Δημόσιο, καθώς ο ίδιος ο οργανισμός θα πρέπει να εγκαταστήσει και να διαχειριστεί τα δικά του κέντρα δεδομένων (datacenters). Στο περιβάλλον αυτό, μετριάζεται το μειονέκτημα της έλλειψης εμπιστοσύνης και της αξιοπιστίας.
- **Κοινοτικό Νέφος** (community cloud): προσιδιάζει σε ένα δημόσιο νέφος, αλλά διαφοροποιείται από αυτό στο επίπεδο της πρόσβασης, καθώς αυτή επιτρέπεται μόνο σε μια συγκεκριμένη κοινότητα καταναλωτών νέφους– οργανισμών, οι οποίοι και μοιράζονται την ευθύνη της ιδιοκτησίας του. Χρησιμοποιείται από πολλές επιχειρήσεις που έχουν κοινούς στόχους και παρόμοιους σκοπούς λειτουργίας, οι οποίες μπορούν να «χτίσουν» ένα κέντρο δεδομένων στο νέφος (πόρους ΤΠ) και κατ’ επέκταση να μοιράζονται τους πόρους του, ως μέλη της. Μπορεί να ανήκει στους ίδιους ή σε κάποιον τρίτο πάροχο δημοσίου νέφους, ο οποίος παρέχει περιορισμένη δυνατότητα

πρόσβασης μόνο στα μέλη της κοινότητας ή ακόμη και μόνο σε συγκεκριμένους πόρους ΤΠ, αυτούς στους οποίους την πρόσβαση επιτρέπει και πάλι η Κοινότητα. Παρέχει μεγαλύτερη εμπιστοσύνη αλλά το βασικό του μειονέκτημα έγκειται στο γεγονός δυσκολίας σύγκλισης απόψεων όλων όσων συμμετέχουν σε αυτό και κατ' επέκταση επίτευξης κοινών όρων και κανονισμών για την εύρυθμη λειτουργία του.

- **Υβριδικό Νέφος** (hybrid cloud): αποτελεί συνδυασμό του ιδιωτικού και του δημόσιου μοντέλου ανάπτυξης νέφους, απαιτώντας διαλειτουργικότητα και δυνατότητα ευελιξίας και μεταφοράς δεδομένων και εφαρμογών, με σκοπό την άμεση επικοινωνία. Κάποια από τα δεδομένα (τα πιο ευαίσθητα και σημαντικά) αποθηκεύονται σε ιδιωτικό νέφος και τα υπόλοιπα σε δημόσιο. Το εν λόγω μοντέλο συνδυάζει τα πλεονεκτήματα του δημόσιου νέφους, δηλαδή το χαμηλό κόστος χρήσης, και του ιδιωτικού, δηλαδή το υψηλότερο επίπεδο ασφάλειας και εμπιστοσύνης.

Ωστόσο, εξαιτίας της ραγδαίας ανάπτυξης της τεχνολογίας αλλά και των απαιτήσεων της αγοράς, έχουν δημιουργηθεί και άλλα παράγωγα μοντέλα όπως λ.χ. το εικονικό ιδιωτικό σύννεφο (virtual private cloud)[13], ή “φιλοξενούμενο νέφος”, το οποίο εκμεταλλευόμενο ένα δημόσιο νέφος, με τρόπο ιδιωτικό–αυτόνομο, επιτυγχάνει τη διασύνδεση όλων των πόρων, παρέχοντας μέσα από ένα εικονικό - ιδεατό ιδιωτικό δίκτυο VPN (Virtuale Private Network)[14] απομόνωση στους χρήστες του. Όποιος το χρησιμοποιεί, εργάζεται σε ένα σχεδόν “ιδιωτικό νέφος”, σαν να μη μοιράζεται δηλαδή την υποδομή του με άλλους χρήστες.

2.3.2 Μοντέλα υπηρεσιών και παράδοσης νέφους[15]

Δύο είναι οι μεγάλες κατηγορίες μοντέλων υπηρεσιών νέφους , τα οποία και προσπαθούν να κατατάξουν οτιδήποτε προσφέρουν οι πάροχοι σαν υπηρεσία ιεραρχικά: το NIST SPI model, μοντέλο τριών επιπέδων υπηρεσιών και το IBM service model, μοντέλο τεσσάρων επιπέδων υπηρεσιών. Οι υπηρεσίες που παρέχει ένα νέφος, διαχωρίζονται από τον εκ των προτέρων συγκεκριμένο παρεχόμενο συνδυασμό πόρων ΤΠ που προφέρει ένας πάροχος, λ.χ. αποθήκευση, υποδομές,

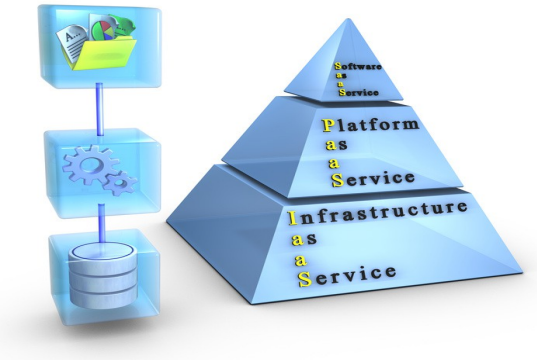
13 Περισσότερες πληροφορίες για το εικονικό ιδιωτικό νέφος βλ. στην ηλ. δ/νση : https://en.wikipedia.org/wiki/Virtual_private_cloud

14 Μέσω ενός προτύπου, ένα τοπικό δίκτυο επιτρέπει την οριοθέτηση μέσα σε αυτό, πολλών εικονικών τοπικών δικτύων – Virtuale Local Area Netoworks, με αποτέλεσμα όσοι κεντρικοί υπολογιστές φιλοξενούνται μέσα σε αυτό να επικοινωνούν μεταξύ τους μέσω μιας εικονικής σύνδεσης (virtuale link- tunnel), μεταξύ δύο κόμβων, δημιουργώντας την ψευδαίσθηση ότι οι κόμβοι αυτοί συνδέονται απευθείας μεταξύ τους χωρίς να παρεμβάλλονται άλλοι . / βλ. Kurose / Ross , Computer net working, a top down approach , sixth edition,, σελ 485, περισσότερα για το VPN βλ και στην ηλ δ/νση https://en.wikipedia.org/wiki/Virtual_private_network

15 Πέρα από τα εδώ περιγραφόμενα μοντέλα, έχουν εμφανιστεί πολλές παραλλαγές τους όπως το Hardware as a Service, Data Base as as Service κ.ά.

λογισμικό κλπ. Τα δύο μοντέλα μεταξύ τους δεν αλληλοσυγκρούονται αλλά αλληλοσυμπληρώνονται. Πιο αναλυτικά :

2.3.2.1 Το NIST SPI model[16]



πήρε το όνομά του από τα αρχικά των λέξεων Service, Platform και Infrastructure και ταξινομεί τις προσφερόμενες υπηρεσίες σε τρία επίπεδα, που δομούνται η μία πάνω στην άλλη:

Το Iaas μοντέλο αποτελεί τη βάση, πάνω στην οποία βασίζονται όλες οι προσφερόμενες υπηρεσίες, με το PaaS να ακολουθεί από πάνω και στην κορυφή της πυραμίδας να βρίσκεται το SaaS.

i) **Software as a service (SaaS) –** λογισμικό ως υπηρεσία: αυτό το μοντέλο απευθύνεται συνήθως σε τελικούς χρήστες– καταναλωτές και η υπηρεσία του αφορά σε ένα πρόγραμμα λογισμικού απομακρυσμένου περιβάλλοντος. Οι χρήστες αποκτούν πρόσβαση σε λογισμικό– σε μία εφαρμογή και βάσεις δεδομένων εφαρμογών, οι οποίες θα έπρεπε να έχουν εγκατασταθεί ή να τρέχουν στον υπολογιστή τους. Οι πάροχοι υπηρεσιών cloud φιλοξενούν, αναπτύσσουν και διαχειρίζονται την υποδομή και τις πλατφόρμες που εκτελούν τις εφαρμογές- “λογισμικό κατά παραγγελία”- με χρέωση ανά χρήση (pay-per-use) ή συνδρομή. Οι πάροχοι είναι αυτοί που εγκαθιστούν και λειτουργούν στο cloud λογισμικό εφαρμογών, στο οποίο έχουν πρόσβαση οι χρήστες του cloud. Οι τελευταίοι περιορίζονται μόνο στη χρήση της παρεχόμενης εφαρμογής και δεν διαχειρίζονται την υποδομή του υπολογιστικού νέφους και την πλατφόρμα όπου εκτελείται η εφαρμογή. Έτσι, εξοικονομούν χρήματα από τη μη ανάγκη αγοράς της υποδομής του λογισμικού αλλά και μνήμη στους υπολογιστές τους. Παραδείγματα, αποτελούν το ηλεκτρονικό ταχυδρομείο, το dropbox, το openoffice κ.ά.

Το **βασικό του μειονέκτημα** έγκειται στην έλλειψη εμπιστοσύνης για τη λήψη των κατάλληλων οργανωτικών και τεχνικών μέτρων ασφαλείας και προστασίας των δεδομένων και πληροφοριών, που λαμβάνει ο πάροχος του νέφους, καθώς όπως προεκτέθηκε, ο χρήστης δεν ασκεί κανένα διαχειριστικό έλεγχο στις υποδομές του νέφους και βασίζεται εξ ολοκλήρου στον πάροχο.

ii) **Platform as a service (PaaS)–** πλατφόρμα ως υπηρεσία[17]: εδώ, ο πάροχος

16 βλ. περισσότερα *Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf , NIST* Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and Technology, Special Publication 500-292 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

17 Thomas Erl, Cloud Computing , Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 68

cloud αναπτύσσει την εργαλειοθήκη, τα πρότυπα και τα κανάλια διανομής και προσφέρει στους προγραμματιστές εφαρμογών– πελάτες / χρήστες του νέφους- ένα "ετοιμοπαράδοτο" περιβάλλον, που τυπικά αποτελείται από ήδη αναπτυγμένους και συγκροτημένους πόρους ΤΠ, όπως πλατφόρμα υπολογιστών, περιβάλλον ανάπτυξης, λειτουργικό σύστημα και περιβάλλον εκτέλεσης γλώσσας προγραμματισμού, web servers. Με αυτό τον τρόπο ο χρήστης αντικαθιστά πλήρως ένα επιτόπιο περιβάλλον (λ.χ πρόσθετοι υπολογιστικοί πόροι, αποθήκευση) και δημιουργεί τις δικές του εφαρμογές (γράφει τον δικό του κώδικα), χωρίς ωστόσο να επιτρέπεται σε αυτόν ο έλεγχος της υποδομής του νέφους.

Μειονέκτημα και εδώ αποτελεί ο ελλιπής έλεγχος που έχει ο ίδιος ο χρήστης. Δηλαδή ο χρήστης περιορίζεται στον έλεγχο της κατασκευαζόμενης από τον ίδιο εφαρμογής, αγνοεί ωστόσο τελείως τι συμβαίνει στο προηγούμενο επίπεδο – IaaS υπηρεσιών και αν ο πάροχος τηρεί τις πολιτικές ασφαλείας ώστε τα δεδομένα να μείνουν απρόσιτα μεταξύ των εφαρμογών. Όλα τα πλεονεκτήματά του, μπορεί να τα εκμεταλλευτεί και ένας ικανότατος hacker για να αναπτύξει ένα κακόβουλο λογισμικό για να επιτεθεί ακόμη και σε έναν ορατό κώδικα που εκτελείται στο περιβάλλον του χρήστη[18].

iii) **Infrastructure as a service (IaaS)–** Υποδομή ως υπηρεσία: με την IaaS παρέχονται στους χρήστες υπολογιστική δομή και εικονικές μηχανές[19]. Πρόκειται συγκεκριμένα για υπηρεσίες online φυσικών υπολογιστικών πόρων, τοποθεσίας, δημιουργίας αντιγράφων ασφαλείας, βιβλιοθήκης δίσκων εικονικής μηχανής, τειχών προστασίας, δεσμών λογισμικού, δικτύου κλπ. Σε αυτό το περιβάλλον νέφους, οι χρήστες αποκτούν ένα υψηλό επίπεδο ελέγχου και ευθύνης επί της παραμετροποίησης και χρησιμοποίησης των πόρων ΤΠ. Η πρόσβαση στους πόρους από τους χρήστες εξακολουθεί να μην είναι άμεση (η υποδομή, οι φυσικοί πόροι, και η παρακολούθηση του δικτύου ανήκουν και διαχειρίζονται από τον πάροχο), ωστόσο δύνανται να επιλέξουν και να ρυθμίσουν τους πόρους που απαιτούνται με βάση τις ανάγκες τους με μία SLA.. Βασίζεται στην εικονικοποίηση.

Φυσικά και αυτό το μοντέλο νέφους έχει τα δικά του **τρωτά σημεία στην ασφάλεια**[20]. Δεδομένου ότι η εικονικοποίηση (virtualization) αποτελεί τον κύριο του

18 HASSAN TAKABI and JAMES B.D., "Security and Privacy Challenges in Cloud Computing Environments", , 2010, διαθέσιμο στην ηλ δ/νση : https://www.researchgate.net/publication/224202015_Security_and_Privacy_Challenges_in_Cloud_Computing_Environments

19 Μία συσκευή παρακολούθησης hypervisor ή εικονικής μηχανής, είναι ένα λογισμικό υπολογιστή, που δημιουργεί και εκτελεί μία ή περισσότερες εικονικές μηχανές που βασίζονται πάνω στον ίδιο υλικό πόρο ΤΠ λ.χ. Linux, και windows μπορούν να εκτελεστούν πάνω σε μία φυσική μηχανή , βλ περισσότερα https://en.wikipedia.org/wiki/Hypervisor

20 Asimi Ahmeda , Tbatou Zakariaea, The 2nd International Workshop on Big Data and Networks Technologies (BDNT'2018) IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors El Balmany Chawkia* , , διαθέσιμο στη ηλ δ/νση : https://ac.els-cdn.com/S1877050918311451/1-s2.0-S1877050918311451-main.pdf?_tid=e9fd7179-6a13-4533-b5c2-608bd8ce0ab8&acdnat=1534954978_aa96e60b7ad957bd5374ed522143ba01

πυρήνα, δημιουργούνται θέματα τόσο από την πλευρά του παρόχου, ο οποίος διαχειρίζεται ολόκληρη την υλική υποδομή και έχει τον πλήρη έλεγχο του hypervisor για την ακρόαση και την επίβλεψη του δικτύου, όσο και από την πλευρά των χρηστών, οι οποίοι πρέπει να λάβουν τα δικά τους κατάλληλα οργανωτικά και τεχνικά μέτρα ώστε να διασφαλίσουν την ασφάλεια του περιβάλλοντός τους από τις απειλές. Η κοινή χρήση των πόρων μπορεί να εκθέσει την ασφάλεια οποιουδήποτε περιβάλλοντος, ακόμη και των φυσικών πόρων του. Επίσης, παρά το απαραίτητο πλεονέκτημα των SLA, δεν υπάρχει κάποια πιστοποίηση για την σωστή εκτέλεση και εκπλήρωση των όρων μιας SLA μεταξύ των εμπλεκομένων μερών. Χρειάζεται υψηλότερη παροχή υπηρεσιών μετρήσεων και μόνιμο έλεγχο της χρήσης του χρήστη. Τέλος δημιουργούνται θέματα ασφάλειας δικτύου.

Αν ένα IaaS περιβάλλον δεν είναι ασφαλές, οι κίνδυνοι που αυτό ελλοχεύει μεταφέρονται και στα ανωτέρω επίπεδα, PaaS και SaaS. Οι Cloud Providers και οι Cloud Consumers σχεδιάζουν, κατασκευάζουν, αναπτύσσουν και λειτουργούν συστήματα που βασίζονται σε cloud. Η διάσπαση του ελέγχου σημαίνει ότι και τα δύο μέρη μοιράζονται τώρα τις ευθύνες όσον αφορά στην παροχή επαρκούς προστασίας στα συστήματα που βασίζονται σε σύννεφο. Η ασφάλεια αποτελεί κοινή ευθύνη[21].

Κατωτέρω παρουσιάζονται γραφικά, δύο πίνακες που συγκρίνουν τα ανωτέρω μοντέλα παράδοσης νέφους, ως προς το επίπεδο ελέγχου και τις δραστηριότητες που εκτελούνται από τους καταναλωτές και του παρόχους τους βλ. [22]:

Μοντέλα παράδοσης νέφους	Τυπικό επίπεδο ελέγχου που εκχωρείται στους καταναλωτές	Τυπική λειτουργικότητα που γίνεται διαθέσιμη σε Καταναλωτή Νέφους
Saas	Συγκρότηση χρησιμοποίησης και σχετιζόμενη με τη χρησιμοποίηση	Πρόσβαση με τοπική διεπαφή χρήστη
Paas	Περιορισμένος διαχειριστικός έλεγχος	Μέτριο επίπεδο διαχειριστικού ελέγχου επί πόρων ΤΠ που σχετίζονται με την χρησιμοποίησης της πλατφόρμας του καταναλωτή νέφους
Iaas	Πλήρης διαχειριστικός έλεγχος	Πλήρης πρόσβαση σε εικονοποιημένους σχετιζόμενους με την υποδομή πόρους ΤΠ και πιθανώς προς του υποκείμενους φυσικούς πόρους ΤΠ

Πίνακας 1. Σύγκριση τυπικών επιπέδων ελέγχου.

21 Βλ NIST cloud computing reference architecture https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

22 βλ. Thomas Erl, Cloud Computing , Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 65

Μοντέλα παράδοσης νέφους	Κοινές δραστηριότητες ΚΑΤΑΝΑΛΩΤΗ νέφους	Κοινές δραστηριότητες ΠΑΡΟΧΟΥ Νέφους
Saas	Χρησιμοποιεί και συγκροτεί υπηρεσία νέφους	Υλοποιεί, διαχειρίζεται και συντηρεί υπηρεσία νέφους παρακολουθεί τη χρησιμοποίηση από καταναλωτές νέφους
Paas	Αναπτύσσει , δοκιμάζει , αναπτύσσει εμπορικά και διαχειρίζεται υπηρεσίες νέφους και βασιζόμενες στο νέφος λύσεις	Συγκροτεί εκ των προτέρων την πλατφόρμα και παρέχει την υποκείμενη υποδομή και άλλους απαραίτητους πόρους ΤΠ, ανάλογα με τις ανάγκες παρακολουθεί τη χρησιμοποίηση από καταναλωτές νέφους
Iaas	Διαμορφώνει και συγκροτεί απογυμνωμένη υποδομή και εγκαθιστά, διαχειρίζεται και παρακολουθεί το τυχόν απαιτούμενο λογισμικό	Παρέχει και διαχειρίζεται τη φυσική απαιτούμενη επεξεργασία, αποθήκευση, δικτύωση και φιλοξενία παρακολουθεί τη χρησιμοποίηση από καταναλωτές νέφους

Πίνακας 2. τυπικές δραστηριότητες που εκτελούνται αντίστοιχα από τους καταναλωτές και παρόχους νέφους.

2.3.2.2 Το IBM service model,

Αυτό το μοντέλο υπηρεσιών, ταξινομεί τις προσφερόμενες υπηρεσίες σε τέσσερα επίπεδα. Τα τρία είναι κοινά με το ως άνω μοντέλο του NIST– SPI. Το επιπλέον επίπεδο υπηρεσίας που παρέχει είναι το **Business Process as a Service– BpaaS**– Υπηρεσία Επιχειρηματικής Διαδικασίας. Σε αυτό, ο πελάτης, είτε είναι απλός χρήστης είτε διευθυντής επιχειρηματικών διαδικασιών, δύναται να σχεδιάζει, να διαχειρίζεται και να ενσωματώνει συνεργατικές διαδικασίες που στηρίζονται στις Saas υπηρεσίες και βρίσκονται ένα επίπεδο παρακάτω, προκειμένου να επιτύχει έναν επιχειρηματικό στόχο, λ.χ. διαδικασίες δοκιμής λογισμικού, διαχείρισης επιδομάτων εργαζομένων κ.ά. Το εν λόγω μοντέλο ταξινομήσει οποιαδήποτε υπηρεσία επιχειρηματικής διαδικασίας, ως BPaaS υπηρεσία, εάν πρόκειται αυστηρά για επιχειρηματική διαδικασία η οποία επιτελείται, μέσα από το υπολογιστικό νέφος και βασίζεται στα κύρια χαρακτηριστικά του, όπως αυτά ορίστηκαν από τον NIST ορισμό. Ο πάροχος είναι ο υπεύθυνος για τις επιχειρηματικές λειτουργίες και προσφέρει τα εργαλεία για την πρόσβαση και αξιοποίηση των πόρων ΤΠ ενώ ο πελάτης δεν είναι ανάγκη να έχει πρόσβαση στα υποκείμενα επίπεδα.

2.4 Πλεονεκτήματα υπολογιστικού νέφους

Ένα από τα σημαντικότερα πλεονεκτήματα της χρήσης του υπολογιστικού νέφους είναι η εξοικονόμηση πόρων και η μείωση του κόστους. Οι χρήστες δύνανται κατ' απαίτηση να έχουν πρόσβαση σε απεριόριστους υπολογιστικούς πόρους και ισχυρή υπολογιστική υποδομή με αναλογικό κόστος (χρέωση ανάλογα με τη χρήση – pay-per-use ή χρονοχρέωση) χωρίς να χρειάζεται να την αγοράσουν οι ίδιοι κάποιο λογισμικό ή να συντηρούν ακριβό εξοπλισμό (διακομιστές, hardware, software) και εγκαταστάσεις αποθήκευσης δεδομένων. Έτσι λ.χ μικρές επιχειρήσεις εξαλείφουν εντελώς ή μειώνουν σημαντικά τις οικονομικές τους υποχρεώσεις, με αποτέλεσμα να διαθέτουν τα κεφάλαια που θα δαπανούσαν για την αγορά υπολογιστικής υποδομής στις κύριες επιχειρηματικές τους επενδύσεις.

Η χρήση του νέφους, επιτρέπει εύκολα και γρήγορα να εργαστεί κανείς και να έχει πρόσβαση στα δεδομένα του και τις εφαρμογές, από οπουδήποτε , οποτεδήποτε και από όποια συσκευή διαθέτει (laptop, desktop, κινητό τηλέφωνο), αρκεί να υπάρχει μία σύνδεση στο Internet.

Επιπρόσθετα, ένα ολοκληρωμένο περιβάλλον νέφους, έχει τη δυνατότητα αυξομείωσης των παρεχόμενων πόρων ΤΠ ανάλογα με τη ζήτηση. Έτσι, σε περίπτωση μη απόκρισης/σφάλματος ή και επίθεσης (π.χ. DoS βλ κατωτέρω ενότητα 2.6.2), ένας εικονικός πόρος ή μια εικονική μηχανή “μεταπηδά” σε ένα εφεδρικό σύστημα, πετυχαίνοντας αξιοπιστία και ελαχιστοποίηση των αστοχιών σε πραγματικό χρόνο εκτέλεσης, άρα ευελιξία στις ανάγκες της υπολογιστικής ισχύος για την εξυπηρέτηση των πελατών του.

Τέλος, ο όγκος των δεδομένων που μπορούν να αποθηκευτούν στο cloud είναι απεριόριστος. Ο οποιοσδήποτε χρήστης μπορεί να διατηρεί αντίγραφα ασφαλείας για όποια και όσα δεδομένα θέλει!

2.5 Μειονεκτήματα και κίνδυνοι στο Υπολογιστικό Νέφος

Όμως, κάθε νόμισμα έχει δύο όψεις. Κατ' επέκταση και in concreto, υπάρχουνε αδυναμίες και ελλοχεύουν σοβαροί κίνδυνοι από τη χρήση του υπολογιστικού νέφους, ιδίως για την προστασία των δεδομένων και το απόρρητο αυτών, με κυριότερους την έλλειψη ελέγχου σε αυτά και την ανεπάρκεια πληροφοριών σχετικά με τον τρόπο με τον οποίο, πού και από ποιον,

(υπό-)εκτελείται η επεξεργασία τους[23]. Οι κίνδυνοι που προσιδιάζουν στο υπολογιστικό νέφος, σχετίζονται με την ίδια τη φύση του, δηλαδή τον κοινόχρηστο χαρακτήρα των πόρων του , την πολυμίσθωση και την ετερογένεια των συστημάτων του. Πιο συγκεκριμένα:

- **Αυξημένη τρωτότητα ασφαλείας[24]**:

Η μεταφορά στο cloud των δεδομένων (προσωπικών ή επιχειρησιακών), ειδικά στα δημόσια νέφη, απαιτεί μία επέκταση των ορίων εμπιστοσύνης καθώς η χρήση πόρων ΤΠ από απόσταση πρακτικά συνεπάγεται τον διαμοιρασμό ή και την εκχώρηση της ευθύνης για την ασφάλειά τους στον πάροχο νέφους, ακόμη και σε τυχόν υπεργολάβους με τους οποίους αυτός συνεργάζεται. Στην πραγματικότητα ο πάροχος έχει απεριόριστη πρόσβαση στα δεδομένα των χρηστών και ο βαθμός ασφαλείας τους, περιορίζεται μόνο στις πολιτικές ασφαλείας και τους μηχανισμούς ελέγχου που εφαρμόζονται θεωρητικά εκατέρωθεν (και από τον χρήστη και από τον πάροχο). Έτσι, ο χρήστης χάνει τον αποκλειστικό έλεγχο των συγκεκριμένων δεδομένων, και αγνοεί πλήρως σε τι είδους επεξεργασία υποβάλλονται αυτά από τους παρόχους, πού αποθηκεύονται, τι είδους μηχανισμοί χρησιμοποιούνται για την προστασία τους, αν τα μέτρα ασφαλείας που λαμβάνει ο πάροχος είναι επαρκή και αν συμμορφώνεται με αυτά. Ως εκ τούτου δεν δύναται να εφαρμόσει ο ίδιος τα κατάλληλα οργανωτικά και τεχνικά μέτρα ασφαλείας που απαιτούνται για τη διασφάλιση της διαθεσιμότητας, της ακεραιότητας, του απορρήτου, της διαφάνειας και της απομόνωσης των δεδομένων.

Επιπρόσθετα, οι πόροι ΤΠ που υπάρχουν σε ένα νέφους επιμερίζονται από κοινού σε διάφορους χρήστες (πολυμίσθωση) και έτσι οι τελευταίοι μοιράζονται τις ίδιες εφαρμογές, λειτουργικό σύστημα και μηχανισμό αποθήκευσης. Ο κάθε χρήστης δεν έχει το δικό του αντίγραφο της εφαρμογής , παρά μόνο ένα στιγμιότυπο αυτής, με αποτέλεσμα να μην υπάρχει επαρκής απομόνωση των δεδομένων[25]. Εύκολα μπορεί κάποιος κακόβουλος ακόμη και χρήστης, να επιτεθεί και στους πόρους του νέφους και στα δεδομένα ενός άλλου χρήστη που βρίσκονται σε αυτούς , βάλλοντας κατά της ακεραιότητας των δεδομένων.

23 Βλ. Ομάδα εργασίας του άρθρου 29 σχετικά με τη νεφοϋπολογιστική, Γνώμη 05/2012 (20-6-2007), διαθέσιμη στην ηλεκτρονική δ/νση: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

24 Thomas Erl, Cloud Computing, Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 45 επ

25 Βλ ENISA, *Cloud Computing Risk Assessment*, December 2012, διαθέσιμο στην ηλεκτρονική δ/νση : https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

- **Μειωμένος έλεγχος λειτουργικής διακυβέρνησης – διαγραφή δεδομένων** [26]

Οι χρήστες του νέφους διαθέτουν χαμηλότερο έλεγχο επί των πόρων ΤΠ του νέφους. Επομένως αγνοούν επαρκείς πληροφορίες σχετικές με το πώς ο πάροχος του νέφους το λειτουργεί, τι εξωτερικές συνδέσεις απαιτούνται για την άμεση μεταξύ τους επικοινωνία (παρόχου – πελάτη) και τη διατήρηση της απόδοσης. Για παράδειγμα, η διαχείριση της υποδομής από τον πάροχο (η χρήση εικονικών μηχανών, η μεγαλύτερη γεωγραφική απόσταση μεταξύ παρόχου και πελάτη που συνεπάγεται πρόσθετα άλματα μέσα στο διαδίκτυο) έχει επίπτωση στην απόδοση των εφαρμογών αλλά συνεπάγεται και μεγαλύτερη έκθεση των δεδομένων που διακινούνται σε αυτό. Ο χρήστης "εμπιστεύεται " τα δεδομένα σε έναν τρίτο– τον πάροχο και στους τυχόν υπεργολάβους του και αμφισβητεί την προστασία τους ή την δυνατότητα διαγραφής– καταστροφής τους[27]. Η απλή εντολή που δίνει κάποιος χρήστης πατώντας το πλήκτρο "delete", δεν αρκεί για την πλήρη διαγραφή των δεδομένων. Σε αυτή την περίπτωση τα δεδομένα, αφήνουν και επομένως εξακολουθούν να υπάρχουν κάποια φυσικά "υπολείμματα" τους, που επιτρέπουν μάλιστα την επαναφορά και την επανάκτησή τους. Η ασφαλής διαγραφή τους προϋποθέτει την επανειλημμένη επανεγγραφή/ αντικατάστασή τους με τυχαίους χαρακτήρες (overwrite) .

Επιπροσθέτως, οι πάροχοι, για να διασφαλίσουν τη διαθεσιμότητα και ακεραιότητα των δεδομένων των χρηστών, δημιουργούν πληθώρα αντιγράφων σε εικονικές μηχανές (VM), ώστε σε περίπτωση αποτυχίας μιας VM, ο πελάτης να ανατρέξει στο αντίγραφο αυτής. Ωστόσο, η ύπαρξη πληθώρας αντιγράφων δημιουργεί εξ ορισμού περισσότερες ευκαιρίες πρόσβασης έστω σε κάποιο από αυτά[28]. Ταυτόχρονα δε, ελλοχεύει κίνδυνος τα αντίγραφα των δεδομένων να εξακολουθούν να υπάρχουν και μετά τον τερματισμό της υπηρεσίας καθώς είναι δύσκολο να εντοπιστούν στο σύνολό τους ώστε να διαγραφούν πλήρως,

Παράλληλα δε ο πάροχος ή οι υπεργολάβοι του μπορεί να μην τηρεί τις εγγυήσεις που ορίζει στη SLA, θέτοντας σε αμφισβήτηση συνακόλουθα και την ποιότητα των λύσεων που δίνει ο ίδιος ο χρήστης , βασιζόμενες σε αυτές.

---

26 Thomas Erl, Cloud Computing , Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 45 επ

27 Η διαγραφή των δεδομένων που έχουν αποθηκευτεί στο cloud, δημιουργεί διάφορα προβλήματα, καθώς αφενός δύναται να έχουν δημιουργηθεί διάφορα αντίγραφα αυτών– απαραίτητη προϋπόθεση για την αποδοτικότητα και διαθεσιμότητα των υπηρεσιών του νέφους- αφετέρου δε, η καταστροφή του φορέα που βρίσκονται αυτά, ελλοχεύει κινδύνους και για τα δεδομένα των άλλων χρηστών, λόγω του χαρακτηριστικού της πολυμίσθωσης του συννέφου. Έτσι, παραβιάζεται το δικαίωμα διαγραφής του υποκειμένου των δεδομένων που ορίζει ο Κανονισμός 2016/679 (ΕΕ), όπως θα αναλυθεί στη συνέχεια.

28 Ειδικά σε περίπτωση που μια VM βρίσκεται σε αδράνεια, ο κίνδυνος καθίσταται μεγαλύτερος καθώς αυτή, δύναται να μην λαμβάνει τα πιο πρόσφατα update ασφάλειας, ώστε να προστατεύεται έναντι κακόβουλων επιθέσεων, βλ. Περισσότερα *Παναγιώτης Παπαδημητρίου*, *Privacy Aspects for Cloud Computing,* Department of Allpied Informatics , University of Macedonia, Greece .

➢ **Περιορισμένη φορητότητα ανάμεσα σε παρόχους νέφους** [29]

Οι πάροχοι δημοσίου νέφους, προσφέρουν προσαρμοσμένες "λύσεις" στις ανάγκες των χρηστών τους, οι οποίες βασίζονται στα δικά τους τεχνολογικά ετερογενή περιβάλλοντα ενώ παράλληλα δεν υπάρχουν καθιερωμένα πρότυπα ανάπτυξης των μοντέλων και των υπηρεσιών τους για την ασφαλή διεπαφή μεταξύ τους και τη φορητότητα των δεδομένων.

Αυτό έχει σαν αποτέλεσμα, ο χρήστης του νέφους να εγκλωβίζεται σε έναν πάροχο (vendor lock-in) και να αδυνατεί να μεταφέρει τα δεδομένα του σε κάποιον άλλο ή να ανταλλάξει πληροφορίες με άλλους χρήστες που χρησιμοποιούν υπηρεσίες νεφοϋπολογιστικής, οι οποίες τελούν υπό τη διαχείριση διαφορετικών παρόχων (διαλειτουργικότητα συστημάτων)[30], γεγονός που μπορεί να συνεπάγεται και πρόσθετες οικονομικές επιβαρύνσεις με την πάροδο του χρόνου για τον πελάτη.

Μάλιστα, όπως θα αναλυθεί στη συνέχεια, αυτή η ενέργεια συνιστά ευθεία παραβίαση του δικαιώματος στη φορητότητα που θεσπίζει ο Νέος Γενικός Κανονισμός για την προστασία των προσωπικών δεδομένων 2016/679/ΕΕ (άρθρο 20 αυτού).

➢ **Οι απαιτήσεις του δικτύου**:

Καθώς η τεχνολογία του υπολογιστικού νέφους βασίζεται και δομείται πάνω σε ένα δίκτυο, ένα έτερο λ.χ μειονέκτημα και απειλή για τη διαθεσιμότητα των δεδομένων[31], συνιστά ακόμη και η τυχαία απώλεια της σύνδεσης δικτύου μεταξύ του πελάτη και του παρόχου ή η διακοπή της εύρυθμης λειτουργίας του διακομιστή λόγω κακόβουλων ενεργειών όπως οι επιθέσεις (κατανεμημένης) άρνησης υπηρεσίας (DoS – βλ κατωτέρω ενότητα 2.6.2). Άλλοι κίνδυνοι που απειλούν τη διαθεσιμότητα είναι οι τυχαίες αστοχίες του υλικού - λογισμικού τόσο στο δίκτυο και στο νεφοϋπολογιστικό σύστημα επεξεργασίας όσο και στο σύστημα αποθήκευσης δεδομένων, οι διακοπές ρεύματος και λοιπά προβλήματα υποδομής[32].

Η μεταφορά των δεδομένων, γίνεται από τον πελάτη προς τους εξυπηρετητές του παρόχου και πίσω, είτε μεταξύ των εξυπηρετητών του παρόχου ή και των

29 Thomas Erl, Cloud Computing , Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 47 επ, και αιτιολογική σκέψη νέου Κανονισμού 2016/679 (ΕΕ) με αρ. 68, όπου αναφέρεται ότι ".... πρέπει να αναπτύσσουν διαλειτουργικούς μορφοτύπους που επιτρέπουν τη φορητότητα"

30 Βλ περισσότερα άρθρο Justice Opara-Martins, Reza Sahandi and Feng Tian, "*Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective*", 2016, διαθέσιμο στην ηλ δ/νση : https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-016-0054-z

31 Διαθεσιμότητα είναι η δυνατότητα απρόσκοπτης και αξιόπιστης πρόσβασης στα δεδομένα ανά πάσα στιγμή.

32 Βλ. Ομάδα εργασίας του άρθρου 29 σχετικά με τη νεφοϋπολογιστική , Γνώμη 05/2012 (20-6-2007), σελ 19, διαθέσιμη στην ηλ. Διεύθυνση http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

υπεργολάβων του, οι οποίοι βρίσκονται σε διαφορετικές περιοχές. Είναι επόμενο λοιπόν να γίνει από κάποιον τρίτο παρακολούθηση των πακέτων του δικτύου (Sniffing[33] ή Spoofing[34] ή του λεγόμενου "Man in the middle"). Τέτοιες "επιθέσεις", ειδικά αν γίνουν από έναν ικανό hacker, που διαγράψει έπειτα τα ίχνη του, είναι δύσκολο να γίνουν αντιληπτές από τον πάροχο του cloud, τη στιγμή που πραγματοποιούνται αλλά και σε δεύτερο χρόνο να εξακριβώσει παράλληλα κατά ποιών δεδομένων έβαλαν[35].

- **Πολυπεριφερειακή συμμόρφωση και νομικά ζητήματα** [36]:

Οι φυσικοί πόροι υποδομής μιας υπηρεσίας νέφους, βρίσκονται διαμοιρασμένοι σε διαφορετικές γεωγραφικά περιοχές με διαφορετική τοπική νομοθεσία, που οι πάροχοι επιλέγουν συνήθως με οικονομικά κριτήρια (φθηνότερες και νομοθετικά πιο ελαστικές). Δηλαδή τα δεδομένα σε περιβάλλον cloud, αποθηκεύονται σε έναν "εκτεθειμένο" και άγνωστο ως τοποθεσία χώρο στους χρήστες. Έτσι, επηρεάζονται από το εκάστοτε τοπικά νομοθετικό πλαίσιο, με αποτέλεσμα να υπάρχει κίνδυνος που αφορά στην πρόσβαση και στην αποκάλυψη των δεδομένων των χρηστών (απόρρητο) σε κυβερνητικές υπηρεσίες ή και σε άλλα πρόσωπα, βάσει αιτημάτων διαφορετικών νομοθετικών καθεστώτων που σύμφωνα με το Δίκαιο της Ένωσης μπορεί να χαρακτηρίζονται και ως "παράνομα".

Για παράδειγμα η Ευρωπαϊκή Ένωση είχε θεσπίσει Οδηγίες, τις οποίες έχουν ενσωματώσει τα κράτη – μέλη, και έχει συνάψει Διεθνείς ή Διμερείς Συμβάσεις με τρίτα κράτη, με στόχο την προστασία των προσωπικών δεδομένων στην υπολογιστική νέφους. Ειδικότερα, η Οδηγίας 95/46/ΕΚ[37], όριζε ότι τα προσωπικά δεδομένα θα πρέπει να αποθηκεύονται είτε στον Ευρωπαϊκό Οικονομικό Χώρο (Ε.Ο.Χ.) ή σε επικράτεια διεπόμενη από ισοδύναμους νόμους περί ιδιωτικότητας (όπου υπάρχουν λ.χ. τυποποιημένες συμβατικές ρήτρες ή δεσμευτικοί εταιρικοί κανόνες, υποχρέωση ειδοποίησης στην αρμόδια εθνική αρχή). Σε αντίθετη

33 Το sniffing περιγράφει την υποκλοπή δεδομένων με τη χρήση ενός ιχνηλάτη (sniffer) που καταγράφει/αιχμαλωτίζει τα πακέτα στη ροή τους στο δίκτυο, / Βλ περισσότερα , edited by James Stanger , Patric T. Lane, *Hack Proofing Linux , The Only Way to Stop a Hacker is to Think Lke One*, 2001, Pages 261-297, Chapter 5 – Troubleshooting the Network with Sniffers, science direct και στην ηλ δ/ νση : https://en.wikipedia.org/wiki/Sniffing_attack .

34 Με τον όρο Spoofing περιγράφεται η επίθεση, κατά την οποία ένα άτομο ή ένα πρόγραμμα μεταμφιέζεται με επιτυχία σε ένα άλλο παραποιώντας τα δεδομένα, για να κερδίσει ένα παράνομο πλεονέκτημα/ βλ περισσότερα Spoofing, στην ηλ δ/ νση, https://en.wikipedia.org/wiki/Spoofing_attack

35 Όπως θα αναλυθεί στη συνέχεια, η παραβίαση των δεδομένων πρέπει να αναφερθεί στην Α.Π.Δ.Π.Χ. εντός 72 ωρών από τη στιγμή που έγινε αντιληπτή και να δοθούν ακριβείς πληροφορίες σχετικά με τη φύση της και τα δεδομένων που δέχθηκαν την επίθεση και άρθρο Bob Duncan , *Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?,*CLOUD COMPUTING 2018 The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization ISBN: 978-1-61208-607-1 ,February 18 - 22, 2018, Barcelona, Spain

36 Thomas Erl, Cloud Computing, Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 48 επ.

37 Πριν αυτή αντικατασταθεί από τον Γενικό Κανονισμό 679/2016/ΕΕ

περίπτωση, ο υπεύθυνος και οι συνυπεύθυνοι της επεξεργασίας και οι εκτελούντες την επεξεργασία πρέπει να προβλέπουν ειδικές εγγυήσεις, καθώς ελλοχεύει ο κίνδυνος να κριθεί κάτι νόμιμο όταν εντός Ε.Ε. θεωρείται παράνομο.

2.6 Ασφάλεια στο υπολογιστικό νέφος (cloud) και απειλές

2.6.1 Η Ασφάλεια στο υπολογιστικό νέφος (cloud)

Η ασφάλεια στο υπολογιστικό νέφος είναι δύσκολο να επιτευχθεί, ακριβώς λόγω του ανοιχτού του περιβάλλοντος και απαιτεί καταρχάς ένα μείγμα τεχνολογιών, τεχνικών ρυθμίσεων και συμπεριφορών, με στόχο την ακεραιότητα των συστημάτων και κατ' επέκταση των δεδομένων. Αφής 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 το πάροχο. Έτσι, ο “ιδιοκτήτης“ των προσωπικών δεδομένων είναι διαφορετικό πρόσωπο από τον “φύλακα” αυτών.

Ένα ασφαλές υπολογιστικό νέφος, μετριέται και διακρίνεται από τα εξής χαρακτηριστικά[38]

ι) **την εμπιστευτικότητα**: 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 διασχίζουν ή βρίσκονται αποθηκευμένα σε αυτό,

ιι) **την ακεραιότητα,** 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).

ιιι) **την 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 κάποια τρίτο μέρος. Αποτελεί σημαντικό χαρακτηριστικό, ειδικά για τις περιπτώσεις που υπάρχει μία διαφωνία σχετική με την ανταλλαγή δεδομένων.

ιϖ) **τη διαθεσιμότητα**: κάθε πότε και για πόσο δύναται ένας χρήστης να έχει πρόσβαση στο νέφος;

Εξ αντιδιαστολής, υπάρχουν και χαρακτηριστικά τα οποία μετρούν την αναξιοπιστία και την έλλειψη ασφάλειας σε ένα cloud:

ι) **η “απειλή”**, δηλαδή μία πιθανή παραβίαση της ασφάλειας με στόχο την

38 Thomas Erl, Cloud Computing, Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 119

παραβίαση ιδιωτικότητας ή/και την πρόκληση βλάβης. Το αποτέλεσμα μιας απειλής που έχει πραγματοποιηθεί καλείται επίθεση.

ιι) **η τρωτότητα**: αυτή αναφέρεται σε μία αδυναμία, που πηγάζει από διάφορες αιτίες, όπως την ανεπάρκεια ελέγχων ασφαλείας, την υπερνίκηση αυτών, ελαττώματα υλικού και λογισμικού, αδυναμίες της πολιτικής ασφαλείας, ανεπάρκεια μέτρων ασφαλείας.

ιιι) **ο κίνδυνος:** είναι η πιθανότητα απώλειας ή βλάβης που προκαλείται από μία απειλή , η οποία έχει εκμεταλλευτεί τις τρωτότητες του cloud.

Επομένως, είναι απαραίτητοι για ένα ασφαλές cloud, οι τακτικοί έλεγχοι, οι μηχανισμοί και πολιτικές ασφαλείας, που σχετίζονται με την λήψη αντιμέτρων για την αποτροπή των απειλών, την αποφυγή ή μείωση των κινδύνων και την υποστήριξη της βέλτιστης ασφάλειας.

2.6.2 Απειλές στην ασφάλεια του υπολογιστικό νέφος (cloud)[39]

Οι πιο συνηθισμένες απειλές που παρατηρούνται σε ένα περιβάλλον cloud είναι οι εξής:

- **η λαθρακρόαση κίνησης - υποκλοπή**: συμβαίνει όταν ένας κακόβουλος πράκτορας υπηρεσίας[40] "κρυφακούει"- υποκλέπτει τα δεδομένα τα οποία βρίσκονται αποθηκευμένα ή διέρχονται από το cloud, με στόχο τη συλλογή πληροφοριών. Προσβάλλεται έτσι η εμπιστευτικότητα των δεδομένων ενώ λόγω της παθητικής της φύσης είναι πιθανό να μην γίνει αντιληπτή εγκαίρως.
- **η απειλή ενός ενδιάμεσου (man in the middle)**: όταν ένας κακόβουλος πράκτορας υπηρεσίας αιχμαλωτίζει τα δεδομένα που διακινούνται στο cloud και αλλοιώνει το περιεχόμενό τους[41], με αποτέλεσμα να βάλλεται η εμπιστευτικότητα και ακεραιότητά τους.
- **η άρνηση υπηρεσίας- DoS** (Denial of Service)[42]: με απλά λόγια αυτή ισοδυναμεί με την συντονισμένη προσπάθεια υπερφόρτωσης των πόρων ΤΠ του υπολογιστικού νέφους, είτε μέσω τεχνητής ή φυσικής αύξησης της ζήτησης

39 Thomas Erl, Cloud Computing, Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας, σελ. 124

40 Κακόβουλος πράκτορας υπηρεσίας είναι ένα άτομο ή ένα πρόγραμμα που μπορεί να αιχμαλωτίσει και να αλλοιώσει το περιεχόμενο των δεδομένων που διακινούνται ή βρίσκονται αποθηκευμένα στο cloud και να προωθήσει εκ νέου την κίνηση το δικτύου, με σκοπό την υποκλοπή τους , την αλλοίωσή τους κ.ά./ βλ Thomas Erl, *Cloud Computing, Αρχές Τεχνολογία & Αρχιτεκτονική*, εκδόσεις Μ. Γκιούρδας, σελ. 126

41 Μπορεί να τροποποιήσει τα απεστελμένα μηνύματα ως προς το περιεχόμενό τους ή να εισάγει και νέα, βλ. περισσότερα Παναγιώτης Παπαδημητρίου, *Privacy Aspects for Cloud Computing, Department of Allpied Informatics*, University of Macedonia, Greece

42 Ως Επίθεση DoS ορίζεται γενικά μία συντονισμένη προσπάθεια να καταστεί ένας υπολογιστής ή μία υπηρεσία ανίκανη να εξυπηρετήσει περισσότερες αιτήσεις από τους εγκεκριμένους χρήστες. Για περισσότερα βλ https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%B9%CE%B8%CE%AD%CF%83%CE%B5%CE%B9%CF%82_%CE%AC%CF%81%CE%BD%CE%B7%CF%83%CE%B7%CF%82_%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%83%CE%B9%CF%8E%CE%BD

των υπηρεσιών του νέφους (π.χ αποστολής πολλαπλών αιτήσεων), ώστε αυτοί να αδυνατούν αν εξυπηρετήσουν τα αιτήματα των πελατών και να καταστούν μη διαθέσιμοι , προσβάλλοντας τη διαθεσιμότητα των δεδομένων.

- **η ανεπαρκής εξουσιοδότηση:** αφορά στην περίπτωση που κάποιος κακόβουλος μη εξουσιοδοτημένος επιτιθέμενος, μπορεί κατά λάθος ή σε ευρεία μορφή να εισέλθει στα δεδομένα τρίτων– ρηστών στο νέφος. Επομένως πολύ σημαντικό ζήτημα αποτελεί και η χρήση ικανών και δύσκολων κωδικών ασφαλείας από τους χρήστες.
- **η επίθεση εικονικοποίησης σε συνδυασμό με την επικάλυψη των ορίων εμπιστοσύνης:** το δημόσιο νέφος έχει τη δυνατότητα να χρησιμοποιεί έναν μόνο φυσικό πόρο ΤΠ για να δημιουργεί πολλούς εικονοποιημένους, ώστε να εξυπηρετεί περισσότερους χρήστες, που προσπελαύνουν το νέφος απομονωμένα μεταξύ τους με τη χρήση ενός hypervisor[43]. Η απόκτηση ελέγχου στον hypervisor, θέτει σε κίνδυνο όλες τις φιλοξενούμενες Vms και κατ' επέκταση παρέχει τα μέσα για την πρόσβαση σε όλα τα δεδομένα που φιλοξενούνται στον συγκεκριμένο διακομιστή cloud, πλήττοντας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων. Οποιαδήποτε ευπάθεια του hypervisor, εκθέτει σε κακόβουλες επιθέσεις όλες τις Vms που αυτός φιλοξενεί και όχι μόνο, καθώς διακινδυνεύουν και οι Vms που διατηρούν δικτυακές συνδέσεις με αυτές που έχουν ήδη δεχθεί επίθεση και φιλοξενούνται από τον host που έχει πληγεί[44].

2.7 Μηχανισμοί Ασφαλείας στο Νέφος

Από τεχνολογικής σκοπιάς, η προστασία και η διασφάλιση της ακεραιότητας των πληροφοριών – δεδομένων, επιχειρείται με διάφορους τρόπους, μεταξύ των οποίων ο έλεγχος και η εξακρίβωση της ταυτότητας του χρήστη κατά την είσοδό του στο cloud (με μηχανισμούς διαχείρισης ταυτότητας - πρόσβασης και αδιάβλητης πιστοποίησης, αυθεντικότητας), η αποστολή ειδοποιήσεων όταν νέες συσκευές ή εφαρμογές συνδέονται στο λογαριασμό, η θέση ψηφιακής υπογραφής στο μήνυμα που περιέχει τα δεδομένα πριν την αποστολή του στο cloud , ο κατατεμαχισμός και η

43 Ο hypervisor (ή αλλιώς virtual machine manager VMM) είναι μία “τεχνική” εικονικοποίησης του υλικού (harware), που απομονώνει τα λειτουργικά συστήματα (Operating Systems-OS) και το λογισμικό (software) από το υποκείμενο υλικό του κεντρικού υπολογιστή (host). Έτσι, το υποκείμενο μηχάνημα του κεντρικού υπολογιστή χειρίζεται ανεξάρτητα μία ή περισσότερες εικονικές μηχανές (Vms- virtual Machines) ως επισκέπτες - guests, επιτρέποντας σε πολλές ταυτόχρονα, να μοιράζονται αποτελεσματικά τους ίδιους φυσικούς υπολογιστικούς πόρους του συστήματος, όπως κύκλους επεξεργαστών, χώρο μνήμης, εύρος ζώνης δικτύου κ.ο.κ, σαν να έχει η κάθε μία τους δικούς της βλ. Περισσότερα στην ηλεκτρονική δ/νση : https://www.techopedia.com/definition/4790/hypervisor ,

44 Παναγιώτης Παπαδημητρίου, *Privacy Aspects for Cloud Computing,* Department of Allpied Informatics , University of Macedonia, Greece

κρυπτογράφηση των δεδομένων πριν αυτά αποθηκευθούν στο cloud.

Η κρυπτογράφηση[45] δύναται να συμβάλει καθοριστικά στην προστασία του απορρήτου των δεδομένων προσωπικού χαρακτήρα, εφόσον εφαρμόζεται με ορθό τρόπο, μολονότι τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται αμετακλήτως ανώνυμα[46]. Η κρυπτογράφηση προτείνεται να χρησιμοποιείται σε όλες τις περιπτώσεις κατά τις οποίες τα δεδομένα "διασχίζουν" το νέφος, και εφόσον είναι διαθέσιμη, όταν τα δεδομένα βρίσκονται σε "αδράνεια". Σε ορισμένες περιπτώσεις (π.χ. υπηρεσία αποθήκευσης IaaS), ο πελάτης υπηρεσιών νεφοϋπολογιστικής δύναται να μην επιλέξει τη λύση της κρυπτογράφησης που προσφέρει ο πάροχος υπηρεσιών νεφοϋπολογιστικής, αλλά να προτιμήσει να προβεί σε κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα προτού τα στείλει στο υπολογιστικό νέφος. Η κρυπτογράφηση των δεδομένων σε αδράνεια απαιτεί ιδιαίτερη προσοχή όσον αφορά στη διαχείριση των κρυπτογραφικών κλειδιών, δεδομένου ότι η ασφάλεια των δεδομένων εξαρτάται ουσιαστικά από την προστασία του απορρήτου των κλειδιών κρυπτογράφησης. Η λύση της κρυπτογράφησης προτείνεται και για την επικοινωνία μεταξύ παρόχου και πελάτη, καθώς και μεταξύ των κέντρων δεδομένων. Σε περίπτωση περαιτέρω επεξεργασίας των δεδομένων προσωπικού χαρακτήρα εντός του υπολογιστικού νέφους (π.χ. αναζήτηση καταχωρήσεων σε βάσεις δεδομένων) από τον πελάτη, πρέπει να σημειωθεί ότι η κρυπτογράφηση δεν μπορεί να διατηρηθεί, με εξαίρεση με περιπτώσεις πολύ ειδικών υπολογισμών[47].

Οι δύο πιο διαδεδομένες μέθοδοι κρυπτογράφησης είναι η συμμετρική και η ασυμμετρική ή κρυπτογράφηση δημόσιου κλειδιού.

Και τα δύο μοντέλα στηρίζονται στο ίδιο πλαίσιο λειτουργίας και επιδιώκουν τον ίδιο στόχο. Δηλαδή: με τον μηχανισμό της κρυπτογράφησης τα απλά και σε αναγνωρίσιμη μορφή δεδομένα που θα αποσταλούν στο νέφος κωδικοποιούνται και μετασχηματίζονται με τη βοήθεια ενός τυποποιημένου αλγορίθμου σε μία μη αναγνωρίσιμη και προστατευμένη μορφή, με στόχο τη διαφύλαξη της ακεραιότητας και της εμπιστευτικότητας αυτών. Τα δεδομένα αποστέλλονται και αποκρυπτογραφούνται με τη βοήθεια ενός μηχανισμού – μιας σειράς αριθμών – που ονομάζεται "κλειδί", το οποίο έχει ο αποστολέας αλλά και πρέπει να γνωρίζει ο παραλήπτης. Όσο μεγαλύτερο είναι το νούμερο των αριθμών που αποτελούν του κλειδί, τόσο μεγαλύτερη και η ασφάλεια που προσφέρει [48].

45 Με απλά λόγια, η Κρυπτογράφηση είναι ένας μηχανισμός που με τη βοήθεια των μαθηματικών μετασχηματίζει σε μη αναγνωρίσιμη μορφή μία ομάδα αναγνωρίσιμων δεδομένων και συμβάλει θεμελιωδώς στην ασφάλεια αυτών.

46 Και γι' αυτό το λόγο εξακολουθούν να είναι προσωπικά δεδομένα. Αν ήταν πλήρως ανωνυμοποιημένα, δεν θα ήταν δυνατό να ταυτιστούν με ένα συγκεκριμένο πρόσωπο και επομένως, δεν θα αποτελούσαν προσωπικά δεδομένα.

47 βλ. Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική- σελ. 20

48 KEITH MARTIN, *Everyday Cryptography*, *Fundamental Principles & Applications*, OXFORD σελ.

- **Συμμετρική κρυπτογράφηση.**

Στη συμμετρική κρυπτογράφηση, χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για τη αποκρυπτογράφηση, το οποίο είναι γνωστό τόσο στον αποστολέα των δεδομένων όσο και στον λήπτη αυτών. Επομένως προϋποτίθεται ότι υπάρχει μεταξύ τους μία σχέση εμπιστοσύνης. Έτσι, ο αποστολέας κρυπτογραφεί τα δεδομένα που θέλει να αποστείλει στο τοπικό περιβάλλον υπολογιστικών του πόρων, τα αποστέλλει , και ο παραλήπτης , που με κάποιο τρόπο γνωρίζει ήδη το κλειδί του αποστολέα, μπορεί να τα αποκρυπτογραφήσει με αυτό. Ωστόσο, επειδή το Διαδίκτυο είναι ένα ανοιχτό και εκτεθειμένο περιβάλλον, δημιουργείται το πρόβλημα της ασφαλούς ανταλλαγής του κλειδιού ανάμεσα στον αποστολέα και τον λήπτη . Πολλές φορές αυτοί οι δύο είναι άγνωστοι μεταξύ τους, οπότε πρέπει να βρεθεί ένα κανάλι ασφαλούς επικοινωνίας, κάτι που δεν διασφαλίζει το Διαδίκτυο.

Παρόλα αυτά, η συμμετρική κρυπτογράφηση είναι ευέλικτη, γρήγορη και αποτελεσματική, καταναλώνει λιγότερη μνήμη και έχει δοκιμαστεί διεξοδικά για πολλές εφαρμογές ασφαλείας σε διάφορες πλατφόρμες[49].

Ο πιο διαδεδομένος αλγόριθμος συμμετρικής κρυπτογράφησης είναι ο AES (Advanced Encryption Data), που μετατρέπει τα δεδομένα σε κωδικοποιημένη μορφή χρησιμοποιώντας “ένα κλειδί” για την αποκρυπτογράφησή τους. Ο AES χρησιμοποιεί μεταβλητό μήκος κλειδιού (128, 192 ή 256 bits) και ανάλογα με το μέγεθος του κλειδιού κρυπτογραφεί και οργανώνει τα δεδομένα σε 10, 12 ή 14 “γύρους”.

- **Ασυμμετρική κρυπτογράφηση ή κρυπτογράφηση δημοσίου κλειδιού.[50]**

Από την άλλη, ο μηχανισμός της ασυμμετρικής κρυπτογράφησης ή κρυπτογράφησης δημόσιου κλειδιού, χρησιμοποιεί δύο κλειδιά ένα δημόσιο και ένα ιδιωτικό, τα οποία αλληλεπιδρούν μεταξύ τους με μία τέτοια μαθηματική συνάρτηση που αφενός μόνο το ιδιωτικό κλειδί μπορεί να αποκρυπτογραφήσει ό,τι το δημόσιο έχει κρυπτογραφήσει και αφετέρου καθίσταται δύσκολο έως αδύνατο, κάποιος που γνωρίζει το δημόσιο κλειδί να μπορεί να ανακαλύψει και το ιδιωτικό . Σε αυτό το μοντέλο, οποιοσδήποτε θέλει να είναι “παραλήπτης” ή “αποστολέας” πρέπει να έχει ένα δικό του ιδιωτικό κλειδί, που θα είναι προστατευμένο και γνωστό αποκλειστικά και μόνο στον ίδιο. Επίσης, θα πρέπει να έχει και ένα δημόσιο κλειδί, το οποίο πρακτικά είναι γνωστό σε ολόκληρη της διαδικτυακή κοινότητα (άρα σε σε κακόβουλους χρήστες / πράκτορες) και επιπλέον συνοδεύεται από κάποιες εγγυήσεις αυθεντικότητας που πιστοποιούν το νόμιμο κάτοχό του. Έτσι, για να στείλει κάποιος

106 επ και KUROSE / ROSS, *Computer Networking A Top-Down Approach*, sixth edition, Chapter 8, σελ. 679 επ.

49 Christos Stergiou a, Kostas E. Psannis a, ⁎, Byung-Gyu Kimb, Brij Guptac, *Secure integration of IoT and Cloud Computing* ,

50 KEITH MARTIN, *Everyday Cryptography*, *Fundamental Principles & Applications*, OXFORD, σελ. 150 επ και KUROSE / ROSS, *Computer Networking A Top-Down Approach*, sixth edition, Chapter 8, σελ. 683 επ.

ένα μήνυμα σε κάποιον άλλο, χρησιμοποιεί το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσει το μήνυμα αυτό. Το κρυπτογραφημένο μήνυμα, μπορεί να αποκρυπτογραφηθεί μόνο με τη χρήση του ιδιωτικού κλειδιού του παραλήπτη στον οποίο φθάνει με εμπιστευτικότητα[51]. Έτσι, με την χρήση δύο κλειδιών αντιμετωπίζεται το πρόβλημα της ασφαλούς ανταλλαγής κλειδιών που παρουσιάζει η σύμμετρη κρυπτογράφηση, όμως τα δύο κλειδιά την καθιστούν σαφώς λιγότερο ευέλικτη και αποδοτική.

Ο RSA αλγόριθμος, είναι ο πιο συνηθισμένος μέχρι στιγμής, αναπτύχθηκε το 1977 από τους Ron Rivest, Adi Shamir και Leonard Adleman, και είναι ο μόνος που χρησιμοποιείται για τη δημιουργία ιδιωτικού και δημόσιου κλειδιού και την κρυπτογράφηση.

Ωστόσο, πάλι δημιουργούνται διάφορα θέματα, τα οποία ερείδονται στο γεγονός ότι σε αυτή τη μέθοδο κρυπτογράφησης το δημόσιο κλειδί είναι γνωστό σε όλους. Έτσι βάλλεται η εμπιστευτικότητα, καθώς οποιοσδήποτε έχει το δημόσιο κλειδί του παραλήπτη, δύναται να προσποιηθεί ότι είναι ο αποστολέας[52]. Επίσης, προβλήματα δημιουργούνται και ως προς την ακεραιότητα και πιστοποίηση της αυθεντικότητας, μιας και οποιοσδήποτε γνωρίζει το δημόσιο κλειδί μπορεί να γράψει κρυπτογραφημένο κείμενο[53].

- **Κατατεμαχισμός (hashing)[54]:**

ένας έτερος μηχανισμός ασφαλείας που χρησιμοποιείται στη νεφοϋπολογιστική για την προστασία της ακεραιότητας των δεδομένων είναι οι συναρτήσεις κατατεμαχισμού (hash functions). Μία hash function είναι μία μαθηματική συνάρτηση, η οποία μετατρέπει τα δεδομένα που εισέρχονται ανεξαρτήτως μεγέθους, σε έναν άλλο αριθμό, που έχει πάντα σταθερό μέγεθος και αντιστοιχεί σε μία μόνο έξοδο/είσοδο. Διακρίνονται για την ανθεκτικότητά τους και την ευκολία στον υπολογισμό, από την σκοπιά της ταχύτητας και της απόδοσης. Επίσης, έχουν ντετερμινιστικά χαρακτηριστικά καθώς το ίδιο ακριβώς μήνυμα, μετατρέπεται και παράγει πάντα την ίδια ακριβώς έξοδο. Οι συναρτήσεις αυτές, χρησιμοποιούνται λ.χ. **i.-** όταν απαιτείται μία μονόδρομη – μη αναστρέψιμη μορφή προστασίας ιδιαίτερα

51 Όπως προαναφέρθηκε, με τον όρο εμπιστευτικότητα εννοείται ότι ο αποστολέας μπορεί να είναι σίγουρος ότι το κρυπτογραφημένο μήνυμα που αποστέλλει στον παραλήπτη, είναι αναγνωρίσιμο μόνο από τον τελευταίο.

52 Το δημόσιο κλειδί του παραλήπτη δεν εγγυάται την πραγματική ταυτότητα του αποστολέα. Εμπιστευτικότητα παρέχεται μόνο ως προς το πρόσωπο του παραλήπτη, ο οποίος είναι και ο μόνος που γνωρίζει το ιδιωτικό κλειδί

53 Περισσότερα για την κρυπτογράφηση δημοσίου κλειδιού, διαθέσιμα και στην ηλ δ/νση https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%94%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D

54 βλ. Thomas Erl, *Cloud Computing, Αρχές Τεχνολογία & Αρχιτεκτονική,* εκδόσεις Μ. Γκιούρδας, σελ. 234

εμπιστευτικών δεδομένων . Αφού εφαρμοστεί ο κατατεμαχισμός σε ένα μήνυμα , αυτό κλειδώνεται και δεν παρέχεται κανένα κλειδί για να το ανοίξει . Η συνηθέστερη εφαρμογή του μηχανισμού αυτού είναι η αποθήκευση των κωδικών πρόσβασης, **ii.-** για να διενεργηθούν έλεγχοι κατά των τυχαίων ή και εσκεμμένων αλλαγών/ τροποποιήσεων των δεδομένων, **iii.-** ως συστατικά για τη δημιουργία άλλων τεχνικών κρυπτογράφησης, **iv.-** ως μέσο "δέσμευσης" των δεδομένων, δηλαδή μέσα σε ένα κρυπτογραφικό πρωτόκολλο για να"δέσει" τα δεδομένα σε μία ενιαία κρυπτογραφημένη "δέσμη", **v.-** ακόμη και για τη δημιουργία κλειδιών κρυπτογράφησης[55].

- **Ψηφιακή υπογραφή[56]:**

Αποτελεί συνονθύλευμα των τεχνολογιών κατακερματισμού και κρυπτογράφησης δημοσίου κλειδιού. Εξασφαλίζει την αυθεντικότητα και την ακεραιότητα των δεδομένων. Τοποθετείται στο μήνυμα πριν την αποστολή του και σε περίπτωση που αυτή υποστεί μη εξουσιοδοτημένες τροποποιήσεις, η ψηφιακή υπογραφή καθίσταται άκυρη.

- **Συστήματα εντοπισμού/πρόληψης εισβολών (IPS/IDS**)[57]

που προλαμβάνουν ή εντοπίζουν απόπειρες παραβίασης των δεδομένων, προκειμένου να επιτευχθεί η απομόνωσή τους[58].

Επιτακτική ωστόσο, καθίσταται η ανάγκη για περαιτέρω έρευνα σε τεχνολογίες ασφάλειας των δεδομένων, καθώς η διαχείριση τεράστιου όγκου δεδομένων (big data), τα οποία προκύπτουν από την ταχεία ανάπτυξη και εκτεταμένη χρήση ψηφιακών αισθητήρων και έξυπνων συσκευών (IoT), είναι αργή και συχνά εγκυμονεί κινδύνους. Οι πλατφόρμες υπολογιστικής νέφους αποτελούν τους πιο πιθανούς "οικοδεσπότες" τους. Αυτό καταδεικνύει ότι, τα συστήματα πιστοποίησης διαδραματίζουν σημαντικό ρόλο διότι διευκολύνουν τους παρόχους να δώσουν αξιόπιστο σήμα στους μελλοντικούς χρήστες ότι συμμορφώνονται προς τα προβλεπόμενα[59] .

---

55 βλ. Keith Martin, *Everyday Cryptygraphy, Fundamental Principles & Applications,* OXFORD, σελ 188 επ.

56 βλ.Thomas Erl, *Cloud Computing, Αρχές Τεχνολογία & Αρχιτεκτονική*, εκδόσεις Μ. Γκιούρδας, σελ. 236

57 Μία συσκευή που παράγει ειδοποιήσεις όταν παρατηρεί μία [ιθανώς κακόβουλη επισκεψιμότητα, καλείται σύστημα ανίχνευσης εισβολής (intrusion detection system- **IDS**), ενώ μία συσκευή που φιλτράρει την πιθανώς ύποπτη κυκλοφορία πακέτων μέσα στο δίκτυο, καλείται σύστημα πρόληψης εισβολής (intrusion prevention system- **IPS**). Τα δύο αυτά συστήματα μαζί ανιχνεύουν την ύποπτη κυκλοφορία. βλ. KUROSE/ ROSS, *Computer Networking A Top-Down Approach*, sixth edition, Chapter 8, σελ. 740 επ. και Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική της Ομάδας του άρθρου 29, της 1ης Ιουλίου 2012, σελ 22

58 Η απομόνωση των δεδομένων καταρχάς προϋποθέτει τη δέουσα διαχείριση δικαιωμάτων και των αρμοδιοτήτων πρόσβασης στα δεδομένα, η οποία πρέπει να επανεξετάζεται τακτικά πχ. δεν πρέπει να επιτρέπεται σε κανέναν χρήστη ή διαχειριστή η πρόσβαση σε ολόκληρο το νέφος.

59 http://europa.eu/rapid/press-release_MEMO-12-713_el.htm

Άλλα μηχανισμοί ασφαλείας στο περιβάλλον του cloud είναι η Υποδομή Δημόσιου κλειδιού, η Διαχείριση Ταυτότητας και Πρόσβασης, η Μοναδική Διαδικασία Αναγνώρισης, οι Βασιζόμενες στο Νέφος Ομάδες Ασφαλείας κ.ά.

2.8 Υπολογιστικό Νέφος και προσωπικά δεδομένα– Γενικοί Προβληματισμοί

Οι κίνδυνοι στο cloud computing , όπως προαναφέρθηκε, πηγάζουν απ' την ίδια τη φύση του και τα χαρακτηριστικά της πολυμίσθωσης, της ετερογένειας των μοντέλων και των προτύπων, του διαμοιρασμού των πόρων του και της τοποθεσίας αυτών και της εικονικοποίησης .

Το πολυδαίδαλο περιβάλλον του συννέφου βρίσκεται μονίμως υπό επίθεση και απειλή. Για παράδειγμα η Yahoo, διαπίστωσε το 2013 1 δισεκατομμύριο παραβιάσεις λογαριασμών χρηστών της, ενώ μόλις πέρυσι που εξαγοράστηκε από τη Verizon, η τελευταία διαπίστωσε ότι το νούμερο των παραβιάσεων για το 2017 ανερχόταν σε 3 δισεκατομμύρια![60]

Ο χρήστης που διαθέτει δεδομένα προσωπικού χαρακτήρα στα συστήματα που τελούν υπό τη διαχείριση παρόχων υπηρεσιών νεφοϋπολογιστικής ενδέχεται να χάνει τον αποκλειστικό έλεγχο των συγκεκριμένων δεδομένων και να μην μπορεί πια να εφαρμόζει τα απαιτούμενα τεχνικά και οργανωτικά μέτρα για τη διασφάλισή τους. Η έλλειψη ελέγχου μπορεί να εκδηλωθεί με διάφορες μορφές λ.χ. έλλειψη διαθεσιμότητας λόγω έλλειψης διαλειτουργικότητας, έλλειψη ακεραιότητας λόγω επιμερισμού των πόρων, μη τήρηση του απορρήτου σε περίπτωση υποβολής αιτημάτων για σκοπούς επιβολής του νόμου απευθείας σε παρόχους υπηρεσιών νεφοϋπολογιστικής, αδυναμία παρέμβασης, έλλειψη απομόνωσης των δεδομένων.

Μέσα σε ένα περιβάλλον cloud υπάρχουν έξι στάδια στον κύκλο ζωής των δεδομένων: η δημιουργία, η αποθήκευση, χρήση, κοινή χρήση, αρχειοθέτηση και καταστροφή και αφής δημιουργηθούν μετακινούνται ελεύθερα ανάμεσα στα υπόλοιπα στάδια. Η προστασία τους λοιπόν, πρέπει να διασφαλίζεται σε ολόκληρο τον κύκλο της ζωής τους και προϋποθέτει την ικανότητα ανίχνευσης της διαδρομής τους[61].

Οι συνήθεις στόχοι της ασφάλειας των δεδομένων είναι η διαθεσιμότητα, η ακεραιότητα και το απόρρητο[62]. Η προστασία των δεδομένων όμως δεν περιορίζεται

60 Bob Ducan,"*Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?*" , CLOUD COMPUTING 2018, The Ninth Conference on Cloud Computing , GRIDs, and Virtualization.

61 βλ. άρθρο *P. Ravi Kumar, P. Herbert Raj, P. Jelciana*, "*Exploring Data Security Issues and Solutions in Cloud Computing",* 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India , science direct

62 βλ. Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική, της 1ης Ιουλίου 2012, σελ 6, διαθέσιμη στην ηλεκτρονική δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-

στην ασφάλειά τους και ως εκ τούτου οι προαναφερθέντες στόχοι συμπληρώνονται με τους ειδικούς στόχους προστασίας των δεδομένων, ήτοι τη διαφάνεια, την απομόνωση, τη δυνατότητα παρέμβασης, τη διαγραφή, τη φορητότητα, έτσι ώστε να υποστηρίζεται πλήρως το δικαίωμα του ατόμου στην προστασία των δεδομένων, το οποίο κατοχυρώνεται στο άρθρο 8 του Χάρτη θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης.

Από την άλλη, οι εταιρίες που χρησιμοποιούν το cloud computing , είτε ως πάροχοι υπηρεσιών νέφος είτε ως κοινωνικά δίκτυα, συγκεντρώνουν καθημερινά τεράστιο όγκο πληροφοριών (big data)[63], όπως το όνομα του χρήστη, τη διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail), τον αριθμό τηλεφώνου του, τη φυσική του διεύθυνση, πληροφορίες σχετικά με τις πληρωμές που έχει πραγματοποιήσει, τη δραστηριότητα του λογαριασμού του (π.χ. κοινοποιήσεις, επεξεργασία, θέαση και μετακίνηση αρχείων ή φακέλων), πληροφορίες σχετικά με τις συσκευές από τις οποίες έκανε χρήση των υπηρεσιών cloud (λ.χ. IP address, τύπος φυλλομετρητή - browser και συσκευής, την ιστοσελίδα που επισκέφθηκε ο χρήστης πριν την επίσκεψή του στην ιστοσελίδα του παρόχου του cloud και την τοποθεσία του εφόσον υπάρχει η σχετική ρύθμιση στη συσκευή του χρήστη), που επεξεργάζονται[64] και συσχετίζουν με το λογαριασμό του κάθε χρήση, χρησιμοποιώντας διάφορες μεθόδους ανάλυσης (π.χ. social network analysis, influence analysis, structural analysis, link analysis κλπ)[65] .

Οι παραπάνω ενδεικτικά αναφερόμενες πληροφορίες είναι δυνατόν να διαβιβάζονται, να αποθηκεύονται και να επεξεργάζονται σε διάφορα μέρη του κόσμου, ακόμη και εκτός της χώρας του χρήστη.

Επίσης, οι εταιρίες πάροχοι υπηρεσιών cloud computing παρέχουν σε τρίτους – υπεργολάβους τη δυνατότητα πρόσβασης και διαμοιρασμού των πληροφοριών των χρηστών που έχουν συλλεχθεί, μολονότι αυτό συνιστά ευθεία παραβίαση της υποχρέωσής τους προς προστασία των δεδομένων των χρηστών. Κατά δήλωσή τους, δεν πωλούν τις πληροφορίες σε διαφημιστές ή τρίτους, αλλά επιτρέπουν σε συγκεκριμένους, οι οποίοι τυγχάνουν της εμπιστοσύνης τους και είναι ρητά εξουσιοδοτημένοι προς τούτο (π.χ. πάροχοι υπηρεσιών υποστήριξης πελατών και

recommendation/files/2012/wp196_el.pdf

63 Κύριο χαρακτηριστικό των big data είναι η δημιουργία και ενσωμάτωση σημαντικού αριθμού δεδομένων, διαφορετικού τύπου, από διαφορετικές πηγές, με τόσο γρήγορο ρυθμό, τον οποίο είναι αδύνατο να εξυπηρετήσουν τα υπάρχοντα συστήματα διαχείρισης δεδομένων. Έτσι, οι πλατφόρμες που βασίζονται στην υπολογιστική νέφους αποτελούν τους πιο πιθανούς “οικοδεσπότες” τους. Η διαχείριση των big data, που προκύπτουν από την ταχεία ανάπτυξη και εκτεταμένη χρήση ψηφιακών αισθητήρων και έξυπνων συσκευών (IoT), είναι αργή και συχνά εγκυμονεί κινδύνους. Αυτό καταδεικνύει ότι, τα συστήματα πιστοποίησης διαδραματίζουν σημαντικό ρόλο διότι διευκολύνουν τους παρόχους να δώσουν αξιόπιστο σήμα στους μελλοντικούς χρήστες ότι συμμορφώνονται προς τα προβλεπόμενα / περισσ. βλ. http://europa.eu/rapid/press-release_MEMO-12-713_el.htm.

64 Σε αυτή την περίπτωση οι εταιρίες είναι υπεύθυνοι επεξεργασίας οι ίδιες, όπως θα αναλυθεί στη συνέχεια.

65 βλ. άρθρο Sapountzi A. – Psannis K., Social networking data analysis tools & challenges

υπηρεσιών της Τεχνολογίας Πληροφοριών) να έχουν πρόσβαση στις πληροφορίες του χρήστη, πραγματοποιώντας ενέργειες για λογαριασμό της εταιρίας, ακολουθώντας την πολιτική απορρήτου της τελευταίας. Σε κάθε περίπτωση, υπεύθυνη για την επεξεργασία των πληροφοριών παραμένει η εταιρία.

Μείζον ζήτημα και ουσιαστική πρόκληση, αποτελεί λοιπόν, η συμμόρφωση με τον Κανονισμό 2016/679 (ΕΕ) για την προστασία των προσωπικών δεδομένων και των χρηστών αλλά και των παρόχων υπηρεσιών νέφους. Επίσης, κρίσιμο είναι το ζήτημα της αποσαφήνισης και αξιολόγησης των ρόλων και των αρμοδιοτήτων που έχει κάθε εμπλεκόμενη οντότητα στο σύνθετο περιβάλλον του cloud, για το προσδιορισμό των υποχρεώσεων που απορρέουν από τη νομοθεσία για την προστασία των δεδομένων σε συνδυασμό με την ενημέρωση και διευκόλυνση των υποκειμένων στην άσκηση των δικαιωμάτων τους.

3 Προσωπικά δεδομένα στο Νέο Γενικό Κανονισμό (ΕΕ) 2016/679 και cloud computing[66]

Στην Ελλάδα, μέχρι πρόσφατα ο νόμος που αφορούσε στην προστασία των προσωπικών δεδομένων και ελευθεριών της ιδιωτικής ζωής των φυσικών προσώπων ήταν ο ν. 2472/1997, που εσωτερίκευσε στην ελληνική έννομη τάξη τη με αριθμό 95/46/ΕΚ οδηγία της Ε.Ε[67] για τα προσωπικά δεδομένα. Πλέον, από 25 Μαΐου 2018, τέθηκε σε εφαρμογή ο Γενικός Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου[68], που κατάργησε την ως άνω Οδηγία, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.

Το νομικό πλαίσιο του Κανονισμού και η συμμόρφωση με αυτόν, δημιουργεί “πονοκέφαλο” τόσο στους CSPs όσο και στους CSCs, αφού η παραβίαση των διατάξεών του επιφέρει βαρύτατες διοικητικές κυρώσεις[69], οι οποίες φθάνουν μέχρι 20.000.000,00 EUR ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους,

66 Στην παρούσα εργασία, δεν θα αναλυθεί ολόκληρο το κείμενο του Κανονισμού 2016/679 (ΕΕ), αλλά οι καινοτομίες του, ως προς τις υποχρεώσεις των υπευθύνων επεξεργασίας και των εκτελούντων αυτή, τα δικαιώματα των υποκειμένων, και οι επιπτώσεις τους στο περιβάλλον του cloud, κατά την κρίση της συγγραφέως.

67 Στις 24 Οκτωβρίου 1995 ψηφίστηκε η Οδηγία 95/46/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (L 281,31) για την προστασία των θεμελιωδών ελευθεριών και δικαιωμάτων των φυσικών προσώπων, και ιδίως της ιδιωτικής ζωής, έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, και την ελεύθερη κυκλοφορία των δεδομένων αυτών.

68 Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (General Data Protection Regulation – GDPR) υπογράφηκε στις 27 Απριλίου 2016 (L 119 της 4-5-2016). Το κείμενο του Κανονισμού είναι διαθέσιμο στην ηλ. διεύθυνση http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679.

69 βλ. Άρθρο 83 Κανονισμού 2016/679 (ΕΕ)

ανάλογα με το ποιο είναι υψηλότερο[70].

Η συμμόρφωση με τον Κανονισμό, προϋποθέτει: σεβασμό των δικαιωμάτων των υποκειμένων, νόμιμη λήψη συγκατάθεσης, νόμιμη βάση επεξεργασίας, τήρηση των υποχρεώσεων του υπεύθυνου επεξεργασίας, λήψη όλων των απαραίτητων οργανωτικών και τεχνικών μέτρων και από τον χρήστη–πελάτη και από τον πάροχο, και ικανότητα απόδειξης όλων των παραπάνω.

3.1 Έννοιες- Ορισμοί

3.1.1 Απλά προσωπικά δεδομένα

Σύμφωνα με το άρθρο 4 του Γενικού Κανονισμού "δεδομένα προσωπικού χαρακτήρα είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό[71] ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου".

Με απλά λόγια, κάθε πληροφορία που αναφέρεται σε συγκεκριμένο φυσικό ζων πρόσωπο[72], του οποίου η ταυτότητα ή είναι γνωστή ή δύναται να εξακριβωθεί αποτελεί προσωπικό δεδομένο. Αν αυτή η πληροφορία πάψει για κάποιο λόγο να συνδέεται με συγκεκριμένο φυσικό πρόσωπο, παύει και να αποτελεί προσωπικό

70 Βλ. Article 29 Data Protection Working Party, Guidelines on the application and setting administrative fines for the purposes of the Regulation 2016/697, adopted on 3 October 2017, διαθέσιμη στην ηλεκτρονική δ/νση : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

71 Ο νέος Κανονισμός διευρύνει την έννοια των προσωπικών δεδομένων. Έτσι στην έννοιά τους εμπίπτουν και τα δεδομένα θέσεως πχ. στίγμα συστήματος γεωεντοπισμού (GPS) και τα επιγραμμικά δεδομένα (δεδομένα σε απευθείας σύνδεση) αποτελούν προσωπικά δεδομένα / βλ. *Φερενίκη Παναγοπούλου – Κουντατζη Ο Γενικός Κανονισμός για την προστασία Δεδομένων 679/2016, Εκδόσεις Σάκκουλα 2017*, σελ. 25 και *ο έλεγχος των εργαζομένων με τεχνικά μέσα : Η περίπτωση του Παγκόσμιου συστήματος γεωγραφικού προσδιορισμού (GPS), Ν.Β. 2012,* σελ 16, Επίσης, προσωπικά δεδομένα αποτελούν διευθύνσεις πρωτοκόλλου internet, αναγνωριστικά cookies κ.ά, τα οποίο αφήνουν ίχνη, ώστε συνδυαζόμενα με άλλα μοναδικά αναγνωριστικά στοιχεία και πληροφορίες που λαμβάνονται από τους διακομιστές, μπορούν να χρησιμοποιηθούν για τη δημιουργία προφίλ των φυσικών προσώπων και να τα αναγνωρίσουν, βλ. αιτιολογική σκέψη 30, βλ επίσης υπόθεση C-582/14 Breyer κατά Γερμανίας ECLI:EU:C:2016:779, όπου το Ευρωπαϊκό Δικαστήριο δήλωσε ότι οι δυναμικές διευθύνσεις IP που διατηρεί ένας διαχειριστής ιστοτόπου συνιστούν δεδομένα προσωπικού χαρακτήρα για όσο διάστημα ο φορέας εκμετάλλευσης ιστοτόπου, διαθέτει μέσα, τα οποία του επιτρέπουν, σε συνδυασμό με άλλες πληροφορίες που έχει ο ISP, τον προσδιορισμό του υποκειμένου των δεδομένων, διαθέσιμη στην ηλ δ/νση : https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=ecli:ECLI:EU:C:2016:779

72 Οι πληροφορίες που αναφέρονται σε νομικά πρόσωπα ή σε θανόντα, δεν αποτελούν προσωπικά δεδομένα.

δεδομένο[73]. Ως εκ τούτου τα ανωνυμοποιημένα δεδομένα, δεν προστατεύονται από τον Γενικό Κανονισμό, καθώς είναι αδύνατη η σύνδεσή τους με κάποιο συγκεκριμένο φυσικό πρόσωπο, σε αντίθεση με τα ψευδωνυμοποιημένα. Επίσης, για να χρήσει εφαρμογής ο Κανονισμός, τα δεδομένα αυτά πρέπει να είναι διαρθρωμένα σε αρχείο[74] .

Έτσι, προσωπικά δεδομένα αποτελούν το όνομα και το επίθετο ενός φυσικού προσώπου, ο αριθμός ταυτότητας, το ΑΜΚΑ του, τα στοιχεία οικογενειακής κατάστασης, οι καταναλωτικές του συνήθειες, τα χόμπι του, τα οικονομικά του στοιχεία, η IP διεύθυνσή του, κ.ά.[75]

3.1.2 Ειδικές κατηγορίες προσωπικών δεδομένων[76]

Ευαίσθητα προσωπικά δεδομένα, αποτελούν αυτά που αποκαλύπτουν τη φυλετική ή εθνιστική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και τα γενετικά και βιομετρικά δεδομένα όταν επεξεργάζονται με σκοπό την αδιαμφισβήτητη ταυτοποίηση του προσώπου, δεδομένα που αφορούν στην υγεία ή τη σεξουαλική ζωή του φυσικού προσώπου ή το γενετήσιο προσανατολισμό αυτού[77] .

Διαφορετικής επίσης μεταχείρισης χρήζουν δεδομένα που αφορούν σε ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφαλείας [78].

3.1.3 Επεξεργασία προσωπικών δεδομένων

Ως επεξεργασία νοείται κάθε πράξη ή σειρά πράξεων πραγματοποιείται από οποιοδήποτε πρόσωπο (φυσικό ή νομικό, ιδιωτικού ή δημοσίου δικαίου, ή ένωση προσώπων), σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, με ή χωρίς τη χρήση αυτοματοποιημένων μέσων. Τέτοιου είδους πράξεις συνιστούν η συλλογή, καταχώρηση, οργάνωση, διάρθρωση, αποθήκευση, προσαρμογή ή μεταβολή, ανάκτηση, αναζήτηση πληροφοριών χρήση, κοινολόγηση με διαβίβαση, διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο

73 Επίσης δεν αποτελούν δεδομένα προσωπικού χαρακτήρα τα στατιστικής φύσης συγκεντρωτικά στοιχεία και οι αξιολογικές ή επιστημονικές κρίσεις (εκτός αν αυτές είναι επίσης λ.χ. Μία ψυχολογική κρίση ή έκθεση αξιολόγησης) , βλ *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Προσωπικά Δεδομένα, σελ. 33

74 Βλ άρθρο 4 στοιχ 6 Γενικού Κανονισμού 2016/679 (ΕΕ) .

75 Περισσότερα για την έννοια των προσωπικών δεδομένων βλ. Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 4/2007 (20-6-2007), διαθέσιμη στην ηλ. δ/νση: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf Βλ. και *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Προσωπικά Δεδομένα, σελ. 43 επ..

76 Βλ άρθρο 9 Γενικού Κανονισμού 2016/679 (ΕΕ).

77 Για τον ορισμό των γενετικών , βιομετρικών δεδομένων και δεδομένων που αφορούν στην υγεία βλ άρθρο 4, στχ 13,14 και 15 αντίστοιχα Γενικού Κανονισμού (ΕΕ) 2016/679

78 Βλ άρθρο 10 Γενικού Κανονισμού 2016/679 (ΕΕ)

συνδυασμός, ο περιορισμός ή διαγραφή ή η καταστροφή (βλ. άρθρο 4 Γενικού Κανονισμού).

Η νομιμότητα της επεξεργασίας κρίνεται και θεμελιώνεται στις αρχές που τη διέπουν και στην προηγούμενη συγκατάθεση του υποκειμένου, αποτελεί δε θεμελιώδη υποχρέωση του υπεύθυνου επεξεργασίας και του εκτελούντος την επεξεργασία.

3.2 Ο υπεύθυνος επεξεργασίας (data controller) και ο εκτελών την επεξεργασία (data processor)

Οι αρμοδιότητες και οι ευθύνες σε περίπτωση πιθανής παραβίασης του Κανονισμού 679/2016 (ΕΕ), πρέπει να κατανέμονται με σαφήνεια, ιδίως σε περίπλοκα περιβάλλοντα επεξεργασίας δεδομένων, όπως όταν αυτή διενεργείται στο ανοιχτό και πολυδαίδαλο περιβάλλον του cloud, όπου εμπλέκονται διάφοροι υπεύθυνοι επεξεργασίας, εκτελούντες την επεξεργασία και υποεκτελούντες αυτήν. Έτσι, αποφεύγεται το ενδεχόμενο υποβάθμισης του επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα ή «αρνητικής σύγκρουσης αρμοδιοτήτων» και εμφάνισης κενών που θα είχαν ως αποτέλεσμα τη μη διασφάλιση από κανένα συμβαλλόμενο μέρος, ορισμένων υποχρεώσεων και κυρίως των δικαιωμάτων των υποκειμένων [79].

Το cloud computing στηρίζεται πάνω σε πολυεπίπεδες και πολύπλοκες δομές επεξεργασίας δεδομένων, σε διάφορες τοποθεσίες ανά τον κόσμο ενώ παράλληλα η επεξεργασία εκτελείται από διάφορα και διαφορετικά πρόσωπα . Ο δε πελάτης, συμβάλλεται μόνο με τον πάροχο της υπηρεσίας που επιθυμεί, αγνοώντας την ύπαρξη ενδιάμεσων – υπεργολάβων του.

3.2.1 Ο υπεύθυνος επεξεργασίας (data controller) – Κανονισμός 2016/679 (ΕΕ)[80].

Υπεύθυνος επεξεργασίας (data controller) είναι το φυσικό ή νομικό πρόσωπο ή δημόσια αρχή, ή υπηρεσία ή άλλος φορέας που (στοιχείο που αφορά στην προσωπική πτυχή του ορισμού), από μόνος του ή από κοινού με άλλους (στοιχείο που αφορά στο ενδεχόμενο πολλαπλού ελέγχου), καθορίζουν τους σκοπούς και τον τρόπο επεξεργασίας δεδομένων προσωπικού χαρακτήρα (βασικό στοιχείο που τον

79 Βλ *Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων*, Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική, της 1ης Ιουλίου 2012, σελ 11, διαθέσιμη στην ηλεκτρονική δ/νση: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

80 Βλ άρθρο 10 Γενικού Κανονισμού 2016/679 (ΕΕ)

διακρίνει από άλλους παράγοντες)[81] και ευθύνεται για την επεξεργασία που πραγματοποιείται ανεξάρτητα αν αυτή εκτελείται από τον ίδιο ή άλλο πρόσωπο .

Δηλαδή, μπορεί να είναι ένας ελεύθερος επαγγελματίας, μία εταιρία, ένα ίδρυμα, ένας δημόσιος οργανισμός, ένας δικηγορικός σύλλογος, μία συνέλευση πολυκατοικίας, ένα Κράτος[82], αλλά όχι ένα φυσικό πρόσωπο κατά την άσκηση δραστηριοτήτων αποκλειστικά προσωπικών ή οικιακών (household excemption)[83].

Σε πολλές περιπτώσεις, πρέπει να αξιολογηθούν οι συμβατικές σχέσεις των διάφορων εμπλεκόμενων μερών, ώστε να εξαχθούν εξωτερικά ασφαλή

81 Όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ευρωπαϊκής 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. Βλ. άρ. 4 αριθμ. 7 Κανονισμού (ΕΕ) 2016/679, Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπεύθυνου επεξεργασίας» και του «εκτελούντος την επεξεργασία» (16-2-2010), διαθέσιμη στην ηλ. διεύθυνση http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

82 Βλ. *Αλεξανδρόπουλου-Αιγυπτιάδου* Ε., Προσωπικά Δεδομένα, σελ. 61 και ΑΠ 2079/2007 ΠοινΧρ 2008.312.

83 Βλ. *Παναγοπούλου-Κουντατζή Φ.*, Περί της προσωπικής-οικιακής χρήσεως των προσωπικών δεδομένων, ΕφΔΔ 2013.704-718. Οι προσωπικές ή οικιακές δραστηριότητες θα μπορούσαν να περιλαμβάνουν την αλληλογραφία και την τήρηση αρχείου διευθύνσεων ή την κοινωνική δικτύωση και την επιγραμμική δραστηριότητα που ασκείται στο πλαίσιο τέτοιων δραστηριοτήτων. Ωστόσο, ο GDPR εφαρμόζεται σε υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία οι οποίοι παρέχουν τα μέσα επεξεργασίας δεδομένων προσωπικού χαρακτήρα για τέτοιες προσωπικές ή οικιακές δραστηριότητες (βλ. αιτιολογική σκέψη αριθμ. 18 Κανονισμού 2016/679). Βλ. την απόφαση C-101/01 του Δ.Ε.Ε. στην υπόθεση Bodil Lindqvist, διαθέσιμη στην ηλ. διεύθυνση http://curia.europa.eu/juris/showPdf.jsf;jsessionid=9ea7d0f130d59241a106d07d43a08f24d75c176244ac.e34KaxiLc3eQc40LaxqMbN4PaN4Me0?text=&docid=48382&pageIndex=0&doclang=el&mode=lst&dir=&occ=first&part=1&cid=672386, η οποία έκρινε ότι «*Η εργασία που συνίσταται στην αναφορά, επί ιστοσελίδας του Διαδικτύου, σε διάφορα πρόσωπα και στον προσδιορισμό τους είτε με το όνομα τους είτε με άλλα μέσα, για παράδειγμα με τον αριθμό τηλεφώνου τους ή με στοιχεία σχετικά με τις συνθήκες εργασίας τους και τις ασχολίες τους κατά τον ελεύθερο χρόνο, συνιστά αυτοματοποιημένη, εν όλω ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα", κατά την έννοια του άρθρου 3, παράγραφος 1, της οδηγίας 95/46 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*», καθώς και ότι η προσωπική ή οικιακή δραστηριότητα «*πρέπει συνεπώς να ερμηνευθεί ως αφορώσα αποκλειστικά τις δραστηριότητες οι οποίες εντάσσονται στο πλαίσιο της ιδιωτικής ή οικογενειακής ζωής των ιδιωτών, πράγμα το οποίο προδήλως δεν ισχύει για την περίπτωση της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, η οποία συνίσταται στη δημοσίευση τους στο Διαδίκτυο με συνέπεια να αποκτά πρόσβαση στα δεδομένα αυτά απροσδιόριστος αριθμός προσώπων*» (σκέψη 47), καθώς και την απόφαση C-212/13 του Δ.Ε.Ε. στην υπόθεση František Ryneš v. Úřad pro ochranu osobních údajů, διαθέσιμη στην ηλ. διεύθυνση http://curia.europa.eu/juris/document/document.jsf?text=131%252F12&docid=160561&pageIndex=0&doclang=EL&mode=req&dir=&occ=first&part=1&cid=533498#ctx1, σύμφωνα με την οποία η χρήση συστήματος με κάμερα, που παρέχει τη δυνατότητα βιντεοσκόπησης προσώπων με αποθήκευση σε μέσο εγγραφής συνεχούς ροής, όπως ο σκληρός δίσκος, το οποίο εγκατέστησε φυσικό πρόσωπο στην κατοικία του με σκοπό την προστασία της ιδιοκτησίας, της υγείας και της ζωής των ιδιοκτητών της οικίας, και το οποίο παρακολουθεί επίσης τον δημόσιο χώρο, δεν συνιστά επεξεργασία δεδομένων η οποία πραγματοποιείται στο πλαίσιο αποκλειστικά προσωπικών ή οικιακών δραστηριοτήτων (σκέψη 35). Βλ. και *Andrade N.*, Oblivion: The Right to Be Different … from Oneself Reproposing the Right to Be Forgotten, "VII International Conference on Internet, Law & Politics. Net Neutrality and other challenges for the future of the Internet" [monograph online], IDP, Revista de Internet, Derecho y Política No. 13, pp. 122-137, Universitat Oberta de Catalunya (Φεβρουάριος 2012), διαθέσιμο στην ηλ. διεύθυνση http://www.raco.cat/index.php/IDP/article/download/251843/337494, σελ. 127-129. Για το εάν ο χρήστης μπορεί να θεωρηθεί υπεύθυνος επεξεργασίας βλ. *Mitrou L./Karyda M.*, EU's Data Protection Reform and the Right to be Forgotten: A Legal Response to a Technological Challenge? (February 5, 2012), 5th International Conference of Information Law and Ethics 2012, Corfu-Greece, June 29-30, 2012, διαθέσιμο στην ηλ. διεύθυνση https://ssrn.com/abstract=2165245, σελ. 9· *Purtova N.*, Property in Personal Data: Second Life of an Old Idea in the Age of Cloud Computing, Chain

συμπεράσματα, αποδίδοντας τον ρόλο και τις αρμοδιότητες του υπευθύνου της επεξεργασίας σε ένα ή περισσότερα μέρη, ανεξάρτητα από τη δύναμη διαπραγματευτικής ισχύος του καθενός. Αυτή η προσέγγιση είναι κρίσιμη, ειδικά σε πολύπλοκα περιβάλλοντα, τα οποία κάνουν χρήση νέων τεχνολογιών των πληροφοριών, όπου οι εμπλεκόμενοι φορείς έχουν συχνά την τάση να αντιλαμβάνονται τον εαυτό τους ως «διαμεσολαβητή» και όχι ως αρμόδιο υπεύθυνο της επεξεργασίας[84].

Για την αποσαφήνιση του ορισμού του υπεύθυνου επεξεργασίας, χρησιμοποιούνται και πραγματολογικά κριτήρια. Έτσι στην πράξη είναι δυνατό να υπάρχουν δύο υπεύθυνοι επεξεργασίας, που η συμμετοχή τους στον κοινό[85] "*καθορισμό* των σκοπών και του τρόπου..." μπορεί να προσλάβει διάφορες μορφές και δεν απαιτείται να είναι επιμερισμένη εξίσου. Επίσης, ως προς την επεξεργασία κάποιων δεδομένων η ίδια οντότητα μπορεί να ενεργεί και ως εκτελών την επεξεργασία αλλά και ως υπεύθυνος επεξεργασίας.

Το βασικότερα χαρακτηριστικό του ορισμού για την αποσαφήνιση του όρου είναι ότι αυτός «*καθορίζει τους στόχους και τον τρόπο*....»[86]. De facto δε, αυτός που ορίζει τον στόχο και ουσιαστικά ζητήματα, σημαντικά για την αξιολόγηση της νομιμότητας της επεξεργασίας όπως π.χ. τα δεδομένα που πρόκειται να υποβληθούν σε επεξεργασία, τη διάρκεια της αποθήκευσης, την πρόσβαση κ.λ.π. Αντίθετα, ο καθορισμός του «τρόπου» της επεξεργασίας μπορεί να μεταβιβασθεί από τον

Informatisation, and Ambient Intelligence (July 16, 2010). TILT Law & Technology Working Paper No. 2010/017, διαθέσιμο στην ηλεκτρονική δ/νση: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1641027, σελ. 9.

84 Μια αρχή προστασίας δεδομένων ασχολήθηκε με τον έλεγχο στο πλαίσιο υπόθεσης καταγγελίας προσώπου στο οποίο αναφέρονταν τα δεδομένα, η οποία αφορούσε αυτόκλητη διαφήμιση μέσω ηλεκτρονικού ταχυδρομείου. Μέσω της καταγγελίας του, το πρόσωπο στο οποίο αναφέρονταν τα δεδομένα ζήτησε από τον πάροχο του δικτύου επικοινωνίας να επιβεβαιώσει ή να αρνηθεί ότι ήταν ο αποστολέας του διαφημιστικού μηνύματος ηλεκτρονικού ταχυδρομείου. Η αρχή προστασίας δεδομένων ανέφερε ότι η εταιρία η οποία παρέχει σε έναν πελάτη μόνο πρόσβαση σε ένα δίκτυο επικοινωνίας, δηλαδή ούτε δρομολογεί τη μετάδοση των δεδομένων ούτε επιλέγει τους παραλήπτες ούτε τροποποιεί τις πληροφορίες που περιέχονται στα δεδομένα που μεταβιβάζονται, δεν μπορεί να θεωρηθεί υπεύθυνος της επεξεργασίας των δεδομένων. βλ. Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία» , της 16ης Φεβρουαρίου 2010, σελ 13 , διαθέσιμη στην ηλ/κη δ/νση: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

85 Η ανταλλαγή δεδομένων ανάμεσα σε δύο μέρη, που αυτά δεν μοιράζονται ούτε τους στόχους ούτε τον τρόπο σε ένα κοινό σύνολο εργασιών, συνιστά απλά διαβίβαση των δεδομένων ανάμεσα σε δύο διαφορετικούς υπεύθυνους επεξεργασίας- βλ Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία» , της 16ης Φεβρουαρίου 2010, διαθέσιμη στην ηλ/κη δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

86 Η ικανότητα να "καθορίζει" μπορεί να πηγάζει από διάφορες νομικές ή/και πραγματικές περιστάσεις: μια ρητή νομική αρμοδιότητα, όταν ο νόμος διορίζει τον υπεύθυνο της επεξεργασίας ή απονέμει ένα καθήκον ή μια υποχρέωση συλλογής και επεξεργασίας ορισμένων δεδομένων αλλά και από πραγματικές αρμοδιότητες ή και άλλα στοιχεία λ.χ. συμβατικές σχέσεις, πραγματικός έλεγχος κλπ- Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία» , της 16ης Φεβρουαρίου 2010, σελ 38, διαθέσιμη στην ηλ/κη δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

υπεύθυνο της επεξεργασίας, όσον αφορά σε επιμέρους τεχνικά ή οργανωτικά ζητήματα στον εκτελούντα την επεξεργασία.

3.2.2 Ο εκτελών την επεξεργασία (data processor)– Κανονισμός 2016/679 (ΕΕ)

Το άρθρο 4 στοιχ. 8 του Κανονισμού 2016/679 (ΕΕ) ορίζει ότι "εκτελών την επεξεργασία" είναι το φυσικό ή νομικό πρόσωπο ή δημόσια αρχή ή άλλος φορέας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου της επεξεργασίας.

Βασικά διακριτικά γνωρίσματα της έννοιας του εκτελούντος την επεξεργασία είναι αφενός ότι η ύπαρξή του εξαρτάται από απόφαση που λαμβάνει ο υπεύθυνος επεξεργασίας, ήτοι τον ορίζει αυτός, και αφετέρου ότι πρόκειται για διαφορετική οντότητα από τον τελευταίο.

Η επεξεργασία από τον εκτελούντα αυτή, προϋποθέτει την ύπαρξη σύμβασης ή άλλης νομικής πράξης υπαγόμενη στο δίκαιο της Ένωσης ή του κράτους μέλους, που τον δεσμεύει σε σχέση με τον υπεύθυνο επεξεργασίας και καθορίζει το αντικείμενο και τη διάρκεια της επεξεργασίας, τη φύση και τον σκοπό της, το είδος των δεδομένων προσωπικού χαρακτήρα, τις κατηγορίες των υποκειμένων των δεδομένων και τις υποχρεώσεις και τα δικαιώματα του εκτελούντος την επεξεργασία[87]

Φυσικά, η επιλογή του γίνεται, σύμφωνα με το άρθρο 28 παρ. 1, μόνο εφόσον παρέχει επαρκείς διαβεβαιώσεις για την εφαρμογή και λήψη κατάλληλων μέτρων (τεχνικών και οργανωτικών, ώστε η επεξεργασία να πληροί τις απαιτήσεις του Κανονισμού 2016/679(ΕΕ). Η τήρηση από μέρους του εγκεκριμένου κώδικα δεοντολογίας ή εγκεκριμένου μηχανισμού πιστοποίησης (σύμφωνα με τα άρθρο 40 και 42 αντίστοιχα), αποτελεί στοιχείο απόδειξης της παροχής των επαρκών διαβεβαιώσεων.

Ο εκτελών την επεξεργασία εκτελεί τις αρμοδιότητες που ο υπεύθυνος επεξεργασίας του έχει ορίσει και για λογαριασμό του τελευταίου, οπότε μπορεί να περιορίζεται σε ένα πολύ συγκεκριμένο καθήκον ή πλαίσιο[88]. Ωστόσο, ο υπεύθυνος

87 Για τους όρους που πρέπει να διαλαμβάνει η σύμβαση μεταξύ υπευθύνου και εκτελούντα την επεξεργασία βλ. άρθρο 28 παρ. 3 Κανονισμού 679/2016 (ΕΕ). Έτσι προκύπτει ότι, ο εκτελών την επεξεργασία θα πρέπει να δεσμεύεται από ειδικές συμβατικές υποχρεώσεις που ορίζει ο υπεύθυνος επεξεργασίας, οι οποίες τον υποχρεώνουν να: διασφαλίζει τη δέσμευση του προσωπικού του ως προς την τήρηση απορρήτου και την εμπιστευτικότητα, να λαμβάνει και αυτός τα κατάλληλα μέτρα προστασία των δεδομένων από τυχούσα απώλεια, αλλοίωση, μη εξουσιοδοτημένη επεξεργασία, να προσλαμβάνει –συνεργάζεται με έτερο υπό – εκτελούντα την επεξεργασία μόνο με την προηγούμενη άδεια του υπεύθυνου επεξεργασίας, να συμφωνεί με τον τελευταίο ως προς τις απαραίτητες τεχνικές και οργανωτικές απαιτήσεις για την εκπλήρωση και διασφάλιση των δικαιωμάτων των υποκειμένων σύμφωνα με τον Κανονισμό 2016/679 (ΕΕ), να βοηθάει τον υπεύθυνο επεξεργασίας κατά την εκπλήρωση της υποχρέωσής του να ειδοποιεί την αρμόδια εποπτική Αρχή ή και τα υποκείμενα των δεδομένων σε περίπτωση παραβίασης αυτών, να παραδώσει όλα τα προσωπικά δεδομένα μετά το πέρας της επεξεργασίας ή της λήξης της σύμβασης παροχής υπηρεσιών .

88 βλ. Άρθρο 28 Κανονισμού 679/2016 (ΕΕ)

επεξεργασίας δύναται να του παραχωρήσει σε ορισμένα θέματα κάποιου είδους διακριτική ευχέρεια, για να εξυπηρετήσει άμεσα συμφέροντά του και να επιτρέπει στον εκτελούντα την επεξεργασία να διατηρεί μία αυτονομία ως προς τον "τρόπο" επεξεργασίας, δηλαδή την επιλογή των κατάλληλων τεχνικών και οργανωτικών μέσων.[89]

Τέλος, για να συνεργαστεί ο εκτελών την επεξεργασία με κάποιον υποεκτελούντα (υπεργολάβο) αυτήν, πρέπει προηγουμένως να λάβει την έγγραφη ειδική ή γενική άδεια του υπεύθυνου επεξεργασίας και οι ίδιες υποχρεώσεις που δεσμεύουν αυτόν (τον εκτελούντα) σε σχέση με τον υπεύθυνο επεξεργασίας, να επιβάλλονται στην έγγραφη σύμβαση μεταξύ αυτού και του υποεκτελούντα[90].

3.2.3 Ο υπεύθυνος επεξεργασίας (data controller) και ο εκτελών την επεξεργασία (data processor) στο υπολογιστικό νέφος

Όπως προεκτέθηκε, για να χαρακτηριστεί κάποιος ως υπεύθυνος επεξεργασίας, αξιολογούνται ο βαθμός λεπτομέρειας καθορισμού των σκοπών της επεξεργασίας και του τρόπου αυτής. Στο περιβάλλον του cloud computing, αυτός είναι καταρχάς ο πελάτης των υπηρεσιών νεφοϋπολογιστικής. Ο πελάτης είναι αυτός που καθορίζει τον τελικό σκοπό της επεξεργασίας και αποφασίζει εν τέλει να την αναθέσει ή όχι και να εκχωρήσει το σύνολο ή μέρος των δραστηριοτήτων της σε εξωτερικό τρίτο οργανισμό – τον πάροχο. Ο πάροχος, παρέχει απλά τα μέσα και την πλατφόρμα και ίσως επιλέγει και τις μεθόδους, τα τεχνικά και οργανωτικά μέσα, προκειμένου ο πελάτης να επιτύχει τους στόχους του και έχει καθήκον να διασφαλίζει το απόρρητο. Επομένως, σε αυτή την περίπτωση ενεργεί εξ ονόματος του εντολέα – πελάτη του και άρα ο πάροχος εν προκειμένω είναι ο εκτελών την επεξεργασία[91].

---

89 Ο "τρόπος" της επεξεργασίας δεν αφορά μόνο στα κατάλληλα τεχνικά μέσα, αλλά και σε οργανωτικά ερωτήματα όπως "πότε θα διαγραφούν κάποια δεδομένα", "ποιοι τρίτοι θα έχουν πρόσβαση" κλπ. , δηλαδή στο "πώς" της επεξεργασίας. Κάποια από αυτά κάλλιστα δύναται να ανατεθούν στον εκτελούντα την επεξεργασία πχ. ποιο λογισμικό ή υλισμικό θα χρησιμοποιηθεί ή ποιος θα έχει πρόσβαση σε αυτά, ερωτήματα που εξ ορισμού πρέπει να απαντώνται από τον υπεύθυνο επεξεργασίας- Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπευθύνου της επεξεργασίας» και του «εκτελούντος την επεξεργασία», της 16ης Φεβρουαρίου 2010, σελ 35, 40, διαθέσιμη στην ηλ/κη δ/νση: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

90 Η CNIL έχει εκδώσει εγχειρίδιο με κατευθυντήριες γραμμές για τον εκτελούντα την επεξεργασία και τη συμμόρφωσή του με τον Κανονισμό 2016/679 (ΕΕ), διαθέσιμο στην ηλ δ/νση: https://www.cnil.fr/en/general-data-protection-regulation-guide-assist-processors

91 Βλ. Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων ,Γνώμη 1/2010 σχετικά με τις έννοιες του υπεύθυνου επεξεργασίας και εκτελούντα την επεξεργασία: "*η ανισότητα διαπραγματευτικής ισχύος μεταξύ ενός μικρού υπεύθυνου της επεξεργασίας δεδομένων και μεγάλων παρόχων υπηρεσιών δεν πρέπει να θεωρείται δικαιολογία για τον υπεύθυνο της επεξεργασίας, ώστε να δεχθεί συμβατικές ρήτρες και όρους οι οποίοι δεν είναι σύμφωνοι προς τη Νομοθεσία για την προστασία των δεδομένων*" και άρθρο 28 Κανονισμού2016/679 (ΕΕ) "ο εκτελών την επεξεργασία", διαθέσιμη στην ηλεκτρονική δ/νση: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_el.pdf

Από την άλλη όμως, ο πάροχος υπηρεσιών υπολογιστικής δύναται να χρησιμοποιεί ο ίδιος δεδομένα για δικούς του σκοπούς (όπως προαναφέρθηκε, οι CSPs συγκεντρώνουν τεράστιο όγκο δεδομένων από διάφορες πηγές που τα επεξεργάζονται και τα συσχετίζουν με το λογαριασμό του κάθε χρήστη), ή σκοπούς διάφορους από αυτούς που όρισε ο πελάτης. Σε αυτή την περίπτωση θεωρείται ο ίδιος υπεύθυνος επεξεργασίας[92]. Επίσης δύναται να είναι από κοινού υπεύθυνος επεξεργασίας και με άλλους παρόχους ή τον πελάτη[93]. Δηλαδή ένας πάροχος νέφους, μπορεί να είναι υπεύθυνος επεξεργασίας ως προς τα δεδομένα που συλλέγει από τους χρήστες του για την εγγραφή τους στην πλατφόρμα υπηρεσιών του (λ.χ. e-mail, ονοματεπώνυμο, ακόμη και δ/νση IP, ώρα εισόδου στην υπηρεσία και διάρκεια παραμονής) αλλά ως προς τα δεδομένα που επιλέγουν οι ίδιοι οι χρήστες να αποθηκεύσουν στην πλατφόρμα του και τα διαχειρίζονται οι ίδιοι, να είναι εκτελών την επεξεργασία.

3.3 Πεδίο Εφαρμογής Κανονισμού 2016/679 (ΕΕ)

Το πεδίο εφαρμογής του Κανονισμού είναι ευρύτατο, αφορά δε και στην μη αυτοματοποιημένη και στην εν όλω ή εν μέρει αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων που οργανώνονται σε ένα σύστημα αρχειοθέτησης[94]. Είναι ένα έξυπνο “νομικό κατασκεύασμα” , με γεωγραφική εμβέλεια σε όλο τον κόσμο, που αποσκοπεί στην προστασία των προσωπικών δεδομένων ανεξάρτητα από τον τόπο στον οποίο αποθηκεύονται ή επεξεργάζονται.

Καταρχάς, εκτείνεται στις δραστηριότητες επεξεργασίας οποιουδήποτε υπεύθυνου επεξεργασίας βρίσκεται εντός της Ε.Ε, αδιάφορου του τόπου όπου αυτή πραγματοποιείται (εντός ή εκτός Ε.Ε.).

Ωστόσο εφαρμόζεται και στην επεξεργασία δεδομένων προσωπικού χαρακτήρα υποκειμένων που βρίσκονται στην Ένωση, από υπεύθυνο επεξεργασίας ή εκτελούντα αυτήν, μη εγκατεστημένο στην Ένωση, εάν εξακριβωθεί ότι αυτοί αποσκοπούν προδήλως να παράσχουν υπηρεσίες που σχετίζονται με την προσφορά αγαθών ή υπηρεσιών στα εν λόγω υποκείμενα των δεδομένων στην Ένωση,

92 Βλ Π. Κίτσος - Π. Παππά, Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους, ΔΙΜΕΕ 2/2012

93 βλ Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων , Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική , της 1ης Ιουλίου 2012, σελ 10, διαθέσιμη στην ηλεκτρονική δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

94 Αρχείο ή σύστημα αρχειοθέτησης αποτελεί κάθε διαρθρωμένο σύνολο δεδομένων προσωπικού χαρακτήρα τα οποία είναι προσβάσιμα με γνώμονα συγκεκριμένα κριτήρια, είτε το σύνολο αυτό είναι συγκεντρωμένο είτε αποκεντρωμένο είτε κατανεμημένο σε λειτουργική ή γεωγραφική βάση (άρθρο 4 στοιχ. 6 Γενικού Κανονισμού)

ανεξαρτήτως εάν απαιτείται πληρωμή από τα υποκείμενα των δεδομένων[95].

Τέλος, βάσεις του άρθρου 3 παρ. 2 στοιχ. β΄ του Κανονισμού, η επεξεργασία δεδομένων προσωπικού χαρακτήρα προσώπων εντός της Ε.Ε., από υπεύθυνο επεξεργασίας ή εκτελούντα αυτήν μη εγκατεστημένο στην Ένωση[96], εμπίπτει στο πεδίο εφαρμογής του και όταν οι δραστηριότητες της επεξεργασίας σχετίζονται με την παρακολούθηση της συμπεριφοράς των υποκειμένων, στο βαθμό που η συμπεριφορά αυτή λαμβάνει χώρα εντός της Ε.Ε. Επομένως, θα πρέπει να εξακριβωθεί κατά πόσον φυσικά πρόσωπα παρακολουθούνται στο Διαδίκτυο, συμπεριλαμβανομένης της δυνητικής μετέπειτα χρήσης 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[97].

Μάλιστα, συσκευές, εφαρμογές, εργαλεία και πρωτόκολλα αυτών, όπως διευθύνσεις διαδικτυακού πρωτοκόλλου, αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων, αποτελούν στοιχεία που συνδέονται με φυσικά πρόσωπα και όταν συνδυαστούν με μοναδικά αναγνωριστικά στοιχεία ταυτότητας και άλλες πληροφορίες που λαμβάνουν οι εξυπηρετητές, μπορούν να χρησιμοποιηθούν για να δημιουργηθεί το προφίλ των φυσικών προσώπων και να αναγνωριστεί η ταυτότητά τους[98].

3.4 Νομιμότητα της επεξεργασίας

Θεμελιώδης υποχρέωση του υπεύθυνου επεξεργασίας αλλά και του εκτελούντα την επεξεργασία είναι η τήρηση των αρχών της και ειδικότερα:

ι) της Αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας[99], σύμφωνα με την οποία τα δεδομένα υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Ειδικότερα, η αρχή της διαφάνειας απαιτεί κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία

95 βλ. Άρθρο 3 παρ. 2 στοιχ α΄ Κανονισμού 2016/679 (ΕΕ) σε συνδυασμό με αιτιολογική σκέψη με αρ. 23 Κανονισμού

96 βλ. άρθρο 27 Κανονισμού 2016/679 (ΕΕ) , σύμφωνα με το οποίο ο υπεύθυνος επεξεργασίας ή ο εκτελών που είναι εγκατεστημένος εκτός της Ε.Ε., πρέπει να ορίσει εγγράφως εκπρόσωπο στην Ένωση, εγκατεστημένο σε ένα από τα κράτη – μέλη όπου βρίσκονται τα υποκείμενα των δεδομένων, των οποίων υποβάλλονται σε επεξεργασία σε σχέση με την προσφορά αγαθών ή υπηρεσιών ή των οποίων παρακολουθείται η συμπεριφορά, προκειμένου να συνεργάζεται με τις αρμόδιες εποπτικές αρχές.

97 βλ. Αιτιολογική σκέψη με αρ. 24

98 βλ. Αιτιολογική σκέψη με αρ. 30

99 αρ. 5 παρ. 1 στοιχ. α' Κανονισμού 2016/679. Η αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας προβλεπόταν και στο προηγούμενο νομοθετικό καθεστώς βλ. άρ. 6 παρ. στοιχ. α' Οδηγίας 95/46/ΕΚ και άρ. 4 παρ. 1 στοιχ. α' ν. 2472/1997

των δεδομένων, τους σκοπούς αυτής[100], τους κινδύνους που εγκυμονεί, το πρόσωπο του υπεύθυνου επεξεργασίας, και τα δικαιώματα του υποκειμένου[101] να είναι εύκολα προσβάσιμη και κατανοητή, διατυπωμένη με σαφήνεια και σε απλή γλώσσα και κατά περίπτωση να υπάρχει σχετική απεικόνιση για την καλύτερη ενημέρωση[102] του υποκειμένου των δεδομένων. Περαιτέρω, το υποκείμενο των δεδομένων θα πρέπει να ενημερώνεται αν καταρτίζεται το προφίλ του και ποιες συνέπειες έχει αυτό[103].

ιι) της αρχής του σαφούς και περιορισμένου σκοπού επεξεργασίας[104],τα δεδομένα δηλαδή δεν πρέπει να υποβάλλονται σε καμιάς μορφής επεξεργασία διαφορετική από αυτή για την οποία συλλέχθηκαν αρχικά. Οι ως άνω σκοποί θα πρέπει να είναι συγκεκριμένοι, νόμιμοι και ρητοί κατά το χρόνο συλλογής των δεδομένων[105].

ιιι) της αρχής της αναλογικότητας και ελαχιστοποίησης των δεδομένων, δηλαδή τα δεδομένα να είναι κατάλληλα , συναφή και να περιορίζονται στο αναγκαίο μέτρο για τους σκοπούς τους οποίους υποβάλλονται σε επεξεργασία[106],

ιϖ) της αρχής της ακρίβειας των δεδομένων: τα δεδομένα πρέπει είναι ακριβή και, όταν είναι αναγκαίο, επικαιροποιούνται· λαμβάνονται δε, όλα τα εύλογα μέτρα για την άμεση διαγραφή ή διόρθωση δεδομένων προσωπικού χαρακτήρα τα οποία

---

100 Οι σκοποί της επεξεργασίας πρέπει να είναι ορισμένοι, πριν τη συλλογή των προσωπικών δεδομένων.

101 βλ. Αιτιολογικές σκέψεις με αρ. 39 , 58 , 59 και 60

102 Όταν οι πληροφορίες παρέχονται στο υποκείμενο ηλεκτρονικά, δηλαδή μέσω μιας ιστοσελίδας, είναι δυνατό οι ως άνω πληροφορίες να αποτυπώνονται και σε εικονίδια, προκειμένου να να δίνεται με ευδιάκριτο, κατανοητό και ευανάγνωστο τρόπο μια ουσιώδης επισκόπηση της σκοπούμενης επεξεργασίας. Αυτό έχει ουσιώδη σημασία στις περιπτώσεις που η πληθώρα των συμμετεχόντων και η πολυπλοκότητα των χρησιμοποιούμενων τεχνολογιών καθιστούν δύσκολο για το υποκείμενο των δεδομένων να γνωρίζει και να κατανοεί εάν, από ποιον και για ποιο σκοπό συλλέγονται δεδομένα προσωπικού χαρακτήρα που το αφορούν, όπως στην περίπτωση επιγραμμικής διαφήμισης ή στην λήψη συγκατάθεσης και ενημέρωσης των παιδιών, βλ. αιτιολογικές σκέψεις με αρ. 58, 59, 60.

103 βλ. Αιτιολογική σκέψη με αρ. 71: Το υποκείμενο θα πρέπει να έχει το δικαίωμα να μην υπόκειται σε απόφαση, η οποία μπορεί να περιλαμβάνει κάποιο μέτρο, με την οποία αξιολογούνται προσωπικές πτυχές που το αφορούν, λαμβανόμενη αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας και η οποία παράγει έννομα αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο, όπως η αυτόματη άρνηση επιγραμμικής αίτησης πίστωσης ή πρακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση. Η επεξεργασία αυτή περιλαμβάνει την «κατάρτιση προφίλ» που αποτελείται από οποιαδήποτε μορφή αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση προσωπικών πτυχών, σχετικά με ένα φυσικό πρόσωπο, ιδίως την ανάλυση ή την πρόβλεψη πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή κινήσεις του υποκειμένου των δεδομένων, στον βαθμό που παράγει νομικά αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο

104Βλ. άρ. 5 παρ. 1 στοιχ. β' Κανονισμού 2016/679 (ΕΕ) // Η εν λόγω αρχή προβλεπόταν και στο προηγούμενο νομοθετικό καθεστώς άρ. 6 παρ. 1 στοιχ. β' Οδηγίας 95/46/ΕΚ και άρ. 4 παρ. 1 στοιχ. α' ν. 2472/1997.

105 βλ. Αιτιολογικές σκέψεις υπ' αρ. 39 και 50 και βλ άρθρο που αφορά στην πρώτη απόφαση Γερμανικού Δικαστηρίου σε εφαρμογή του Κανονισμού 2016/679 (ΕΕ), διαθέσιμο άρθρο στην ηλ δ/νση : https://www-compliancejunction-com.cdn.ampproject.org/c/s/www.compliancejunction.com/first-gdpr-ruling-issued-in-german-courts/amp/

106 Άρ. 5 παρ. 1 στοιχ. γ' Κανονισμού 2016/679 και άρ. 6 παρ. 1 στοιχ. γ' Οδηγίας 95/46/ΕΚ και άρ. 4 παρ. 1 στοιχ. β' ν. 2472/1997

είναι ανακριβή, σε σχέση με τους σκοπούς της επεξεργασίας[107]

ϖ) της αρχής του καθορισμού της χρονικής διάρκειας της επεξεργασίας- "περιορισμός της περιόδου αποθήκευσης"[108], σύμφωνα με την οποία τα δεδομένα διατηρούνται υπό μορφή που επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων μόνο για το διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας[109]

ϖι) της αρχής της ακεραιότητας και εμπιστευτικότητας[110]: τα δεδομένα υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια των δεδομένων προσωπικού χαρακτήρα, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων και

ϖιι) της αρχής της λογοδοσίας (accountability): Την ευθύνη και το βάρος απόδειξης της συμμόρφωσης με τις ως άνω αναφερόμενες αρχές και λήψης των κατάλληλων και αποτελεσματικών μέτρων για την εφαρμογή τους, φέρει ο υπεύθυνος επεξεργασίας (άρθρο 5 παρ. 2 Κανονισμού)[111].

Στις ΤΠ, όπου πελάτες, πάροχοι υπηρεσιών νεφοϋπολογιστικής και υπό-εκτελούντες την επεξεργασία, δύνανται να φέρουν ο καθένας κάποιο μερίδιο επιχειρησιακής ευθύνης, ως λογοδοσία νοείται η ικανότητα μιας οντότητας να αποδεικνύει τι έκανε, με ποιον τρόπο και σε ποια χρονική στιγμή στο παρελθόν. Επομένως, κατ' επέκταση, η ικανότητα μιας πλατφόρμας υπολογιστικού νέφους να παρέχει αξιόπιστους μηχανισμούς παρακολούθησης και ολοκληρωμένης καταγραφής

107 Άρ. 5 παρ. 1 στοιχ. δ' Κανονισμού 2016/679, άρ. 6 παρ. 1 στοιχ. δ' Οδηγίας 95/46/ΕΚ και άρ. 4 παρ. 1 στοιχ. γ' ν. 2472/1997. Βλ. *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Προσωπικά Δεδομένα, σελ. 79-8

108 Βλ. άρ. 5 παρ. 1 στοιχ. ε' Κανονισμού 2016/679, άρ. 6 παρ. 1 στοιχ. ε' Οδηγίας 95/46/ΕΚ και άρ. 4 παρ. 1 στοιχ. δ' ν. 2472/1997. Η τήρηση της αρχής της καθορισμένης χρονικής διάρκειας διατήρησης των δεδομένων ικανοποιεί το δικαίωμα του υποκειμένου να περιπίπτουν σε λήθη τα προσωπικά του δεδομένα, όταν παύουν να εξυπηρετούν το σκοπό της επεξεργασίας βλ. *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Προσωπικά Δεδομένα, Νομική Βιβλιοθήκη (2016), σελ. 82 επ..

109 Τα δεδομένα προσωπικού χαρακτήρα μπορούν να αποθηκεύονται για μεγαλύτερα διαστήματα, εφόσον θα υποβάλλονται σε επεξεργασία μόνο για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, σύμφωνα με το άρθρο 89 παράγραφος 1 και εφόσον εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα που απαιτεί ο Κανονισμός για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων

110 Άρ. 5 παρ. 1 στοιχ. στ' Κανονισμού 2016/679.

111 Στα κοινά μέτρα λογοδοσίας μπορούν να περιλαμβάνονται ενδεικτικά : α) η θέσπιση εσωτερικών διαδικασιών πριν από τη δημιουργία νέων εργασιών επεξεργασίας δεδομένων προσωπικού χαρακτήρα (εσωτερικός έλεγχος, αξιολόγηση κ.λ.π.), β) θέσπιση γραπτών και δεσμευτικών πολιτικών προστασίας δεδομένων, γ) η χαρτογράφηση διαδικασιών ώστε να διασφαλίζεται κατάλληλη αναγνώριση όλων των εργασιών επεξεργασίας δεδομένων και διατήρηση καταλόγου εργασιών επεξεργασίας δεδομένων, δ) ο διορισμός υπεύθυνου για την προστασία των δεδομένων, ε) η παροχή κατάλληλης εκπαίδευσης και κατάρτισης στους υπαλλήλους για την προστασία των δεδομένων, στ) η θέσπιση διαδικασιών για τη διαχείριση των αιτημάτων πρόσβασης, διόρθωσης και διαγραφής, που πρέπει να είναι διαφανή για τα άτομα στα οποία αναφέρονται τα δεδομένα, ζ) η εγκαθίδρυση εσωτερικού μηχανισμού χειρισμού καταγγελιών, η) η θέσπιση εσωτερικών διαδικασιών για την αποτελεσματική διαχείριση και αναφορά παραβιάσεων ασφαλείας και θ) η διενέργεια αξιολόγησης του αντικτύπου στην ιδιωτική ζωή σε ειδικές περιπτώσεις - Βλ. αναλυτ. Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας (13-7-2010), διαθέσιμη στην ηλ. διεύθυνση http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_el.pdf

της κίνησης στο νέφος της ώστε ανά πάσα στιγμή να είναι σε θέση ο πάροχος να απαντήσει στα ως άνω ερωτήματα.

Ο Colin Bennett[112] διακρίνει τρία επίπεδα λογοδοσίας : της πολιτικής, των διαδικασιών και της πρακτικής. Οι πρώτοι δύο τύποι λογοδοσίας αντιστοιχούν στηνύπαρξη κατάλληλων εγγράφων που καθορίζουν τις πολιτικές απορρήτου που εφαρμόζει το σύστημα, δηλαδή την τεκμηρίωση των απαιτήσεων προστασίας της ιδιωτικής ζωής και των εσωτερικών μηχανισμών και διαδικασιών (όπως η PIA, η διαδικασία χειρισμού καταγγελιών, η κατάρτιση του προσωπικού κ.λ.π.). Ο τρίτος τύπος λογοδοσίας είναι πιο απαιτητικός: για να συμμορφώνονται με την υποχρέωση λογοδοσίας όσον αφορά στην εφαρμογή στην πράξη, οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να είναι σε θέση να αποδείξουν ότι ο πραγματικός χειρισμός των δεδομένων τους συμμορφώνεται με τις υποχρεώσεις τους. Αυτό προϋποθέτει την τήρηση ημερολογίων ελέγχου και αρχείων καταγραφής, τα οποία πρέπει επίσης να συμμορφώνονται με άλλες αρχές προστασίας της ιδιωτικής ζωής, όπως η αρχή της ελαχιστοποίησης των δεδομένων[113].

Έτσι οι πάροχοι θα έπρεπε να παρέχουν έγγραφα από τα οποία να προκύπτει και αποδεικνύεται ότι λαμβάνουν όλα τα προσήκοντα και αποτελεσματικά μέτρα που εγγυώνται την επίτευξη των στόχων των βασικών αρχών προστασίας των δεδομένων όπως οι διαδικασίες αναγνώρισης όλων των μηχανισμών επεξεργασίας των δεδομένων, οι διαδικασίες απάντησης σε αιτήματα πρόσβασης , η κατανομή των πόρων, συμπεριλαμβανομένου του καθορισμού υπεύθυνου προστασίας των δεδομένων κ.ά, ώστε οι υπεύθυνοι επεξεργασίας να είναι πάντοτε έτοιμοι να καταδεικνύουν στην αρμόδια εποπτική αρχή κατόπιν σχετικού αιτήματος τα αναγκαία μέτρα που ελήφθησαν.[114,]

112 Καθηγητής Τμήματος Πολιτικών Επιστημών στο Πανεπιστήμιο της Βικτώρια, περισσότερα βλ. https://www.uvic.ca/socialsciences/politicalscience/people/directory/bennettcolin.php

113 βλ. ENISA , *Privacy and Data Protection by Design - from policy to engineering* –December 2014, σελ 21, διαθέσιμο στην ηλεκτρονική δ/νση: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

114 Λογοδοσία σημαίνει ότι απαραίτητη προϋπόθεση για τη αποτελεσματική εποπτεία των δεδομένων, είναι η τήρηση ορισμένων βασικών δεικτών απόδοσης (key performance indicators (KPIs), της επεξεργασίας από τους παρόχους υπηρεσιών νέφους στη βάση των εντολών που έλαβαν από τον πελάτη Ένας υπεύθυνος επεξεργασίας δύναται να είναι αποτελεσματικά υπεύθυνος, μόνο εάν μπορεί να αποδείξει με κάποιον μετρήσιμο τρόπο ότι συμμορφώνεται με τον Κανονισμό, διαφορετικά η αρχή της λογοδοσίας δεν μπορεί να εκπληρωθεί σωστά. Έτσι, ο πελάτης – υπεύθυνος επεξεργασίας πρέπει να έχει ένα δικαίωμα ελέγχου σε διάφορες φάσεις της επεξεργασίας, για να είναι σε θέση να αντιληφθεί και να αντιμετωπίσει τους κινδύνους που συνδέονται με κάποια πράξη αυτής ή τη φύση της. Μεταφράζεται δε σε δικαίωμα να ελέγξει τη θέση των διακομιστών όπου επεξεργάζονται/ αποθηκεύονται τα δεδομένα, δικαίωμα ελέγχου του λογικού (αλγόριθμοι) που χρησιμοποιείται κατά τη διάρκεια διάφορων ενεργειών που προβλέπονται για το σύνολο της επεξεργασίας , δικαίωμα ελέγχου των μέτρων ασφαλείας που εφαρμόζει ο πάροχος νέφους – εκτελών την επεξεργασία κλπ/ βλ. Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική , της 1ης Ιουλίου 2012, σελ 22, διαθέσιμη στην ηλεκτρονική δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

3.5 Δικαιώματα υποκειμένου

Ο υπεύθυνος επεξεργασίας οφείλει να διευκολύνει την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων και να λαμβάνει τα κατάλληλα μέτρα για να παρέχει στο υποκείμενο κάθε πληροφορία και ανακοίνωση σχετικά με τη διενεργούμενη από αυτόν επεξεργασία σε συνοπτική, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή, χρησιμοποιώντας σαφή και απλή διατύπωση, ιδίως όταν πρόκειται για πληροφορία απευθυνόμενη ειδικά σε παιδιά[115] (άρθρο 12 παρ. 2 και παρ. 1 εδ. α' Κανονισμού). Οι πληροφορίες παρέχονται γραπτώς ή με άλλα μέσα (π.χ. ηλεκτρονικώς, εφόσον ενδείκνυται), αλλά και προφορικά, εφόσον η ταυτότητα του υποκειμένου των δεδομένων είναι αποδεδειγμένη με άλλα μέσα (άρθρο 12 παρ. 1 εδ. β' και γ' Κανονισμού).

Τα δικαιώματα του υποκειμένου των δεδομένων , που προβλέπονται στον Κανονισμό 2016/679 (ΕΕ) είναι:

ι) το δικαίωμα της ενημέρωσης[116] και πρόσβασης στα δεδομένα[117], που ορίζει την υποχρέωση του υπεύθυνου επεξεργασίας για μεγαλύτερη και σαφέστερη ενημέρωση του υποκειμένου κατά τη συλλογή των δεδομένων και την πρόσβαση σε αυτά[118],

ιι) το δικαίωμα διόρθωσης, που αφορά στη διόρθωση ανακριβών στοιχείων δεδομένων ή συμπλήρωση ελλιπών δεδομένων που αφορούν το υποκείμενο[119]

115 Βλ. αναλυτ. *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Κοινωνία της πληροφορίας και νομική προστασία των προσωπικών δεδομένων της οικογένειας και των μελών της, ΕλλΔνη 2008.691-699· *ίδια*, Η πλοήγηση των ανηλίκων στο διαδίκτυο και η νομική προστασία των προσωπικών δεδομένων, Αρμ 2007.848-854· ίδια, *Η προστασία των προσωπικών δεδομένων ανηλίκων στον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679* ,ΔΙΜΕΕ 1/2018 , Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 2/2009 για την προστασία προσωπικών δεδομένων παιδιών (γενικές κατευθυντήριες γραμμές και η ειδική περίπτωση των σχολείων) (11-2-2009), σελ. 15, διαθέσιμη στην ηλ. δ/νση http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_el.pdf

116 Βλ. Άρθρα 13 και 14 Κανονισμού 2016/679 (ΕΕ) και αναλυτ. *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Προσωπικά Δεδομένα, σελ. 133-138 και *Τουντόπουλο Β.*, Το δικαίωμα ενημέρωσης του υποκειμένου των δεδομένων, ΔΕΕ 1999.576 επ..

117 βλ. Άρθρο 15 Κανονισμού 2016/679 (ΕΕ) και αναλυτ. *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Προσωπικά Δεδομένα, σελ. 138-141. Βλ. επίσης υπ' αριθμ. 89/2017 και 89/2013 αποφάσεις Α.Π.Δ.Π.Χ.· ΣτΕ 1662/2017 ΤΝΠ ΝΟΜΟΣ· ΣτΕ 4597/2015 ΤΝΠ ΝΟΜΟΣ.

118 Βλ απόφαση 33/2018 ΑΠΔΠΧ, με την οποία απηύθυνε σύσταση σε Τράπεζα, η οποία προέβη σε τιτλοποίηση και μεταβίβαση χαρτοφυλακίου δανείων και πιστώσεων σε οριστική καθυστέρηση σε άλλη εταιρία, διότι στο κείμενο του υποβληθέντος σχεδίου ενημέρωσης των υποκειμένων ΔΕΝ αναφέρονταν με σαφήνεια οι κατηγορίες των απαιτήσεων που έχουν τιτλοποιηθεί (π.χ. όλες οι καταγγελθείσες συμβάσεις μέχρι μια συγκεκριμένη ημερομηνία και οι ληξιπρόθεσμες απαιτήσεις από τις είκοσι δανειακές συμβάσεις που θα αναφέρονται μόνο με τον αριθμό τους) προκειμένου τα υποκείμενα των δεδομένων να είναι σε θέση να αναγνωρίσουν ευχερώς ότι τους αφορά, και β) δεν αποσαφηνιζόταν σε ποιον υπεύθυνο επεξεργασίας μπορούν να απευθύνονται τα υποκείμενα των δεδομένων προκειμένου να ασκήσουν τα δικαιώματα πρόσβασης και αντίρρησης αναφορικά με την τιτλοποίηση και τη διαχείριση των απαιτήσεων, αλλά αντ' αυτού η εν λόγω τράπεζα στο ως άνω κείμενο γνωστοποίησης– ενημέρωσης των υποκειμένων περιορίστηκε απλά στην γενική και ασαφή διατύπωση του εξής: «20 ληξιπρόθεσμων για τα οποία είχαν ληφθεί αποφάσεις καταγγελίας με ημερομηνία 31.03.2017 δανείων και πιστώσεων», χωρίς δηλαδή να αναφέρονται οι μοναδικοί αριθμοί ή άλλα προσδιοριστικά στοιχεία των σχετικών συμβάσεων, ώστε τα υποκείμενα των δεδομένων να μπορούν να αναγνωρίσουν ευχερώς ότι τα αφορά.

119 βλ. Άρθρο 16 Κανονισμού 2016/679 (ΕΕ) .

ιιι) το δικαίωμα περιορισμού της επεξεργασίας, που όταν ασκηθεί υποχρεώνει τον υπεύθυνο της επεξεργασίας υπό προϋποθέσεις[120] να περιορίσει την επεξεργασία αυτών,

ιϖ) το δικαίωμα εναντίωσης[121], του άρθρου 21 του Κανονισμού, ορίζει ότι το υποκείμενο των δεδομένων δύναται να αντιταχθεί στην επεξεργασία αυτών, υπό προϋποθέσεις, και ιδίως όταν πρόκειται για "κατάρτιση προφίλ" ή για σκοπούς απευθείας εμπορικής προώθησης,

ϖ) το δικαίωμα διαγραφής[122]: Εάν το υποκείμενο ασκήσει το δικαίωμα διαγραφής (right to erasure ή άλλως το δικαίωμα στη λήθη στο ψηφιακό περιβάλλον[123]) των προσωπικών δεδομένων που το αφορούν, ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει τα προσωπικά δεδομένα[124] χωρίς αδικαιολόγητη καθυστέρηση, εφόσον ισχύει ένας τουλάχιστον από τους περιοριστικά αναφερόμενους στη διάταξη του άρθρου 17 παρ. 1 Κανονισμού 2016/679 λόγους

Όταν ο υπεύθυνος επεξεργασίας υποχρεούται να διαγράψει προσωπικά δεδομένα τα οποία έχει ήδη δημοσιοποιήσει, οφείλει, λαμβάνοντας υπόψη τη διαθέσιμη τεχνολογία και το κόστος εφαρμογής, να λαμβάνει εύλογα μέτρα, συμπεριλαμβανομένων των τεχνικών μέτρων, για να ενημερώσει τους υπεύθυνους επεξεργασίας (εκτελούντες, και αποδέκτες) που επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, ότι το υποκείμενο των δεδομένων ζήτησε τη διαγραφή από αυτούς (ενν. τους υπευθύνους επεξεργασίας) τυχόν συνδέσμων με τα δεδομένα αυτά ή αντιγράφων ή αναπαραγωγών των εν λόγω δεδομένων προσωπικού χαρακτήρα (άρθρο 17 παρ. 2 Κανονισμού)[125], εκτός αν αυτό αποδεικνύεται ανέφικτο ή εάν συνεπάγεται δυσανάλογη προσπάθεια (άρθρο 19 Κανονισμού).

120 βλ. Άρθρο 18 Κανονισμού 2016/679 (ΕΕ)

121 Στο ν. 2472/1997 γινόταν λόγος για το δικαίωμα αντίρρησης - βλ. αναλυτ. *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Προσωπικά Δεδομένα, σελ. 142 επ.· *ίδια*, Ηλεκτρονική επεξεργασία προσωπικών δεδομένων και το δικαίωμα αντίρρησης του υποκειμένου τους, Αρμ 2005.137-142. Στο δε άρ. 14 Οδηγίας 95/46/ΕΚ προβλέπεται το δικαίωμα αντίταξης (βλ. σχετ. *Hoboken JVJ*, The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment (Ιούνιος 2013), διαθέσιμο στην ηλ. διεύθυνση http://www.law.nyu.edu/sites/default/files/upload_documents/VanHoboken_RightTo%20Be%20Forgotten_Manuscript_2013.pdf

122 Βλ. αναλυτ *Παναγοπούλου – Κουτνατζή Φ.*, Η εξέλιξη του δικαιώματος στη λήθη (περί λήθης της λήθης;), ΕφημΔΔ 2016.714-728-. *Γκαγκάτση Α.*, Το δικαίωμα στην ψηφιακή λήθη στη διεθνή έννομη τάξη (2014), διπλωματική εργασία, διαθέσιμη στην ηλ. Διεύθυνση: http://ikee.lib.auth.gr/record/135622/files/GRI-2014-13587.pdf·

123 Ο νομοθέτης δεν ταυτίζει ορολογικά τη διαγραφή με τη λήθη. Το προστατευόμενο δυνάμει του άρ. 17 δικαίωμα συνίσταται σε ένα δικαίωμα διαγραφής, το οποίο έχουμε συνηθίσει να αποκαλούμε – ανακριβώς- δικαίωμα στη λήθη, γι' αυτό και ο δεύτερος αυτός όρος τέθηκε εντός παρενθέσεως. Βλ. *Παναγοπούλου – Κουτνατζή Φ.*, Η εξέλιξη του δικαιώματος στη λήθη (περί λήθης της λήθης;), ΕφημΔΔ 2016.714-728(718-719) και *Ιωάννης Δ. Ιγγλεζάκης* , Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του, εκδόσεις Σάκκουλα 2014

124 Για τον τρόπο πραγματοποίησης της διαγραφής βλ. την υπ' αριθμ. 1/2005 Οδηγία της ΑΠΔΠΧ για την ασφαλή καταστροφή των προσωπικών δεδομένων μετά το πέρας της περιόδου που απαιτείται για την πραγματοποίηση του σκοπού της επεξεργασίας ή γενικότερα της περιόδου τήρησης των προσωπικών δεδομένων, διαθέσιμη στην ηλ. Διεύθυνση http://www.dpa.gr/portal/page?_pageid=33,120908&_dad=portal&_schema=PORTAL

125 Βλ. και αιτιολογική σκέψη αριθμ. 67 Κανονισμού 2016/679.

Έτσι, ο πελάτης του cloud – υπεύθυνος επεξεργασίας θα ενημερώσει τον πάροχο – εκτελούντα, ο οποίος με τη σειρά του θα ενημερώσει τυχόν υπεργολάβους του – υποεκτελούντες , σχετικά με το αίτημα του υποκειμένου για την πλήρη διαγραφή των δεδομένων του. Ήδη όμως αναφέρθηκε, ότι οι τελικοί χρήστες υπηρεσιών cloud δυσπιστούν ως προς την ικανότητα του παρόχου για την πλήρη διαγραφή των δεδομένων τους, από οποιοδήποτε υλικό φορέα (υπάρχουν αντίγραφα ασφαλείας για να διασφαλίζεται η αδιάλειπτη παροχή της υπηρεσίας)[126], μιας και ζούμε στην εποχή της απόλυτης ψηφιακής μήνης[127].

ϖι) το δικαίωμα στη φορητότητα των δεδομένων (data portability)[128]: Το υποκείμενο των δεδομένων, όταν η επεξεργασία τους βασίζεται στη συγκατάθεσή του ή σε σύμβαση, δικαιούται είτε να λαμβάνει τα δεδομένα που το αφορούν σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνωρίσιμο από μηχανήματα μορφότυπο, είτε να ζητάει την απευθείας διαβίβασή τους από τον ένα υπεύθυνο επεξεργασίας στον άλλο, άρα από τον ένα πάροχο στον άλλο, και ο τελευταίος υποχρεούται να το πράξει χωρίς αντίρρηση, εφόσον ωστόσο είναι τεχνικά εφικτό.

Ο Κανονισμός 2016/679/ΕΕ, καταρχάς, δεν υποχρεώνει τους παρόχους cloud να αναπτύξουν διαλειτουργικά τεχνικά συστήματα συμβατά μεταξύ τους, παρά μόνο τους ενθαρρύνει. Παράλληλα, ορίζει ότι όταν σε συγκεκριμένο σύνολο δεδομένων θίγονται περισσότερα του ενός υποκείμενα δικαιωμάτων, η άσκηση του εν λόγω δικαιώματος δεν θα πρέπει να θίγει τα δικαιώματα και τις ελευθερίες των άλλων υποκειμένων[129].

Ωστόσο, για την άσκηση του δικαιώματος της φορητότητας σε τεχνικό επίπεδο[130], οι υπεύθυνοι επεξεργασίας θα πρέπει να υιοθετήσουν διάφορους

126 Η απλή εντολή που δίνει κάποιος χρήστης πατώντας το πλήκτρο “delete”, δεν αρκεί για την πλήρη διαγραφή των δεδομένων , αφήνουν και επομένως εξακολουθούν να υπάρχουν κάποια φυσικά “υπολείμματα” τους , που επιτρέπουν μάλιστα την επαναφορά και την επανάκτησής τους. Η ασφαλής διαγραφή τους προϋποθέτει την επανειλημμένη επανεγγραφή/ αντικατάστασή τους με τυχαίους χαρακτήρες (overwrite)

127 βλ. Απόφαση (c-131/12) ECLI:EU:C:2014:317 Google Spain SL, Google Inc. Κατά Agencia Española de Protección de Datos (AEPD), Mario Costeja González, διαθέσιμη στην ηλ δ/νση: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EL&mode=lst&dir=&occ=first&part=1&cid=498704, η οποία αναγνωρίζει το δικαίωμα (πριν την εφαρμογή του Κανονισμού 2016/679 (ΕΕ), των υποκειμένων να ζητούν από τους φορείς παροχής υπηρεσιών μηχανών αναζήτησης στο διαδίκτυο, τη διαγραφή αποτελεσμάτων αναζήτησης που περιέχουν προσωπικά τους δεδομένα

128 Βλ. Άρθρο 20 Κανονισμού 2016/679 (ΕΕ) και περισσότερα Article 29 Data Protection Working Party, Guidelines on the right to data portability, adopted on 13 December 2016, όπως αναθεωρήθηκε και υιοθετήθηκε στις 5 Απριλίου 2017, διαθέσιμο στην ηλ. διεύθυνση http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf

129 Βλ. Αιτιολογική σκέψη 68 του Κανονσιμού 2016/679 (ΕΕ).

130 βλ. Article 29 Data Protection Working Party, Guidelines on the right to data portability, adopted on 13 December 2016, όπως αναθεωρήθηκε και υιοθετήθηκε στις 5 Απριλίου 2017, σελ. 5, διαθέσιμη στην ηλεκτρονική δ/νση : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

τρόπους για την υλοποίησή του π.χ μέσω δυνατότητας απευθείας λήψης (download) του συνόλου των δεδομένων ή μιας διεπαφής προγραμματισμού εφαρμογών API[131].

Με αυτό το ρητό δικαίωμα ενδυναμώνεται η θέση του υποκειμένου των δεδομένων – χρήστη αναφορικά με το πρόβλημα της μειωμένης διαλειτουργικότητας (vendor lock – in), που αναλύθηκε σε προηγούμενη ενότητα (βλ. ενότητα 2.5 *Μειονεκτήματα υπολογιστικού νέφους – περιορισμένη φορητότητα ανάμεσα στους παρόχους νέφους*) .

3.6 Βασικές υποχρεώσεις υπεύθυνου επεξεργασίας

Ο Κανονισμός 2016/679 (ΕΕ) ενισχύει τα δικαιώματα των υποκειμένων και μέσα από την αύξηση των υποχρεώσεων του υπεύθυνου επεξεργασίας[132].
Οι βασικές του υποχρεώσεις είναι:

- **Η λήψη κατάλληλων τεχνικών και οργανωτικών μέτρων**, ώστε να μπορεί να διασφαλίζει και να αποδεικνύει ότι η επεξεργασία των δεδομένων, διενεργείται σύμφωνα με τα όσα ορίζει ο Κανονισμός[133], τα οποία επανεξετάζονται και επικαιροποιούνται,
- **Κατάρτιση πολιτικής ασφαλείας και κωδίκων δεοντολογίας**[134],
- **Η τήρηση αρχείου δραστηριοτήτων** για τις οποίες είναι υπεύθυνος, σε φυσική ή ηλεκτρονική μορφή[135],
- **Η διενέργεια εκτίμησης αντικτύπου (Data Protection Impact Assessment- DPIA)** και προηγούμενη διαβούλευση[136], κυρίως για επεξεργασία δεδομένων που παρουσιάζουν υψηλό κίνδυνο και αφορούν στην αξιολόγηση

131 Το API είναι ένα ενδιάμεσο λογισμικό που επιτρέπει την επικοινωνία μεταξύ δύο εφαρμογών , βλ. περισσότερα στην ηλ. δ/νση : https://el.wikipedia.org/wiki/Διεπαφή_προγραμματισμού_εφαρμογών.
Μάλιστα, απόρροια της ραγδαίας ανάπτυξης της τεχνολογίας είναι και η δημιουργία των λεγόμενων APIs πολλών συννέφων (multi-cloud APIs), τα οποία παρέχουν μία ενιαία διεπαφή ανεξάρτητη από την εξειδικευμένη πλατφόρμα cloud, βλ. *Reginaldo Rea,, Romulo Manciola Melocaa, Douglas Nassif Roma Juniorb, Marcelo Alexandre da Cruz Ismaelc, Gabriel Costa Silva*, "An Empirical Study for Evaluating the Performance of Multi-cloud APIs" , άρθρο Science Direct

132 βλ. *Φερενίκη Παναγοπούλου – Κούτνατζη,* ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ, εκδόσεις Σάκκουλα 2017, σελ 31.

133 βλ. άρθρο 24 Κανονισμού 2016/679/ΕΕ

134 βλ. άρθρο 40 Κανονισμού 2016/679/ΕΕ // Η αιτιολογική σκέψη 99 EU του Κανονισμού, ενθαρρύνει τους ιδιωτικούς φορείς για την κατάρτιση κώδικα δεοντολογίας ή την τροποποίηση ή επέκταση ενός ήδη υφιστάμενου, να διαβουλεύονται με τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένων των υποκειμένων των δεδομένων όπου αυτό είναι εφικτό, και να λαμβάνουν υπόψη τις παραληφθείσες παρατηρήσεις και τις απόψεις που εκφράζονται σε απάντηση διαβουλεύσεις – διαθέσιμη στην ηλ. δ/νση https://gdpr-info.eu/recitals/no-99.

135 βλ. Άρθρο 30 Κανονισμού 2016/679 (ΕΕ), δυνάμει του οποίου θεμελιώνεται το πρώτον η εν λόγω υποχρέωση για τήρηση αρχείου από τον υπεύθυνο επεξεργασίας (και από τον εκτελούντα την επεξεργασία) και *Παναγοπούλου – Κουτνατζή Φ.*, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ, σελ. 33.

136 βλ. Άρθρο 35 Κανονισμού 2016/679 (ΕΕ)

προσωπικών πτυχών, σε δεδομένα μεγάλης κλίμακας ή σε παρακολούθηση δημοσίου χώρου. Η εν λόγω υποχρέωση θα αναλυθεί κατωτέρω, στην 4η ενότητα της παρούσας εργασίας.

❖◑ **Προστασία εξ ορισμού και από τον σχεδιασμό (Privacy by design and by default).**

Το απόρρητο της επεξεργασίας των προσωπικών δεδομένων πρέπει να διασφαλίζεται με αυστηρούς μηχανισμούς ασφάλειας, φυσικής και ηλεκτρονικής[137]. Μία έτερη βασική υποχρέωση του υπεύθυνου επεξεργασίας ορίζεται στο άρθρο 25 και αφορά στην προστασία των δεδομένων ήδη από τον σχεδιασμό (privacy by design)[138] και εξ ορισμού (privacy by default)[139].

Συγκεκριμένα, όπως προβλέπεται στο άρθρο 25 παρ. 1 Κανονισμού 2016/679/ΕΕ, ο υπεύθυνος επεξεργασίας, λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων από την επεξεργασία, οφείλει να εφαρμόζει αποτελεσματικά, τόσο κατά τη στιγμή του καθορισμού των μέσων επεξεργασίας όσο και κατά τη στιγμή της επεξεργασίας, κατάλληλα τεχνικά και οργανωτικά μέτρα, όπως η ψευδωνυμοποίηση, σχεδιασμένα για την εφαρμογή αρχών προστασίας των δεδομένων, όπως η ελαχιστοποίηση των δεδομένων, και την ενσωμάτωση των απαραίτητων εγγυήσεων στην επεξεργασία κατά τρόπο ώστε να πληρούνται οι απαιτήσεις του Κανονισμού και να προστατεύονται τα δικαιώματα των υποκειμένων των δεδομένων[140].

Επίσης, οφείλει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει ότι, εξ ορισμού, υφίστανται επεξεργασία μόνο τα προσωπικά δεδομένα που είναι απαραίτητα για τον εκάστοτε σκοπό της επεξεργασίας. Αυτή η υποχρέωση ισχύει για το εύρος των προσωπικών δεδομένων που συλλέγονται, το βαθμό της επεξεργασίας τους, την περίοδο αποθήκευσης και την προσβασιμότητά τους. Συγκεκριμένα, με τη λήψη των εν λόγω μέτρων διασφαλίζεται ότι, εξ ορισμού, τα δεδομένα προσωπικού χαρακτήρα δεν καθίστανται προσβάσιμα χωρίς την

137 βλ αναλυτικότερα *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Προσωπικά Δεδομένα, σελ. 129.

138 Βλ. αναλυτ. European Union Agency for Network and Information Security (ENISA), *Privacy and Data Protection by Design – from policy to engineering* (Δεκέμβριος 2014), διαθέσιμο στην ηλ. δ/νση https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design *Μήτρου Λ.*, Privacy by Design – Η τεχνολογική διάσταση της προστασίας προσωπικών δεδομένων, ΔiMEE 2013.14-25.

139 Βλ. *Φερενίκη Παναγοπούλου – Κουτνατζή Φ.*, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ, σελ. 32.

140 Ο υπεύθυνος επεξεργασίας μπορεί να αναθέτει την επεξεργασία σε πρόσωπα που τελούν υπό τον απόλυτο έλεγχό του και ενεργούν μόνο κατ' εντολή του. Τα πρόσωπα αυτά επιλέγονται βάσει των επαγγελματικών τους προσόντων, παρέχοντας έτσι εγγυήσεις για την ύπαρξη τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου/βλ. αναλυτ. *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*,Προσωπικά Δεδομένα, σελ.129.

παρέμβαση του φυσικού προσώπου σε αόριστο αριθμό φυσικών προσώπων[141].

Η συμμόρφωση του υπεύθυνου επεξεργασίας με την προστασία των προσωπικών δεδομένων ήδη από το σχεδιασμό και εξ ορισμού μπορεί να αποδεικνύεται μέσω εγκεκριμένου μηχανισμού πιστοποίησης (άρθρο 25 παρ. 3 σε συνδυασμό με άρθρο 42 Κανονισμού).

Στο περιβάλλον των υπολογιστών και των δικτύων η διασφάλιση του απορρήτου μεταφράζεται σε υιοθέτηση τεχνικών μηχανισμών που καλούνται Τεχνολογίες Ενίσχυσης της Ιδιωτικότητας – Privacy Enhancing Technologies (PETs)[142], όπως η κρυπτογράφηση[143], διάφορα πρωτόκολλα για ανώνυμες επικοινωνίες, οι μηχανισμοί αδειοδότησης και αδιάβλητης πιστοποίησης (π.χ. έλεγχος γνησιότητας με δύο παράγοντες), ο έλεγχος ταυτότητας χρήστη, η ιδιωτική αναζήτηση σε βάση δεδομένων, μηχανισμοί ειδοποίησης σε περίπτωση παραβίασης, η ψευδωνυμοποίηση κ.ά., που αφορούν στην πρόληψη της παραβίασης. Μία έκθεση της ENISA, που πραγματεύεται το τι πρέπει να γίνει προκειμένου να επιτευχθεί το Privacy by design and by default, ορίζει π.χ. ότι οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης πρέπει να διενεργούνται σε τοπικό επίπεδο, και όχι μέσω μιας απομακρυσμένης υπηρεσίας, προκειμένου να διασφαλίζεται η μυστικότητα των κλειδιών και η ασφάλεια των δεδομένων. Επίσης, τονίζει ότι η εξωτερική αποθήκευση δεδομένων σε ένα απομακρυσμένο cloud μπορεί να είναι ασφαλής αρκεί τα κλειδιά της αποκρυπτογράφησης να τα έχει μόνο ο ιδιοκτήτης των δεδομένων (ή ο υπεύθυνος επεξεργασίας) και όχι και ο πάροχος[144].

Αυτό σημαίνει ότι ο πελάτης των υπηρεσιών νεφοϋπολογιστικής οφείλει να αξιολογεί αν ο πάροχος που επιλέγει λαμβάνει τα ως άνω τεχνικά μέτρα, αν αυτά είναι αποτελεσματικά και διαλειτουργικά. Επίσης οφείλει να εξακριβώνει ότι παρέχει στα υποκείμενα των δεδομένων τη δυνατότητα παρέμβασης σε τεχνικό και οργανωτικό επίπεδο για την άσκηση των δικαιωμάτων τους ακόμη και στις περιπτώσεις που αυτά, υφίστανται μεταγενέστερη επεξεργασία από υπεργολάβους.

---

141 Άρ. 25 παρ. 2 Κανονισμού 2016/679.

142 βλ. Περισσότερα , ENISA, "*Privacy and Data Protection by Design – from policy to engineering"* – December 2014, διαθέσιμο στην ηλεκτρονκή δ/νση : https://publications.europa.eu/en/publication-detail/-/publication/6548a14b-9863-410d-a8a6-c15a0137d281/language-en

143 Η επικοινωνία μεταξύ των κέντρων δεδομένων, προτείνεται να είναι κρυπτογραφημένη. Η εξ αποστάσεως διαχείριση της πλατφόρμας υπολογιστικού νέφους προτείνεται να γίνεται μόνο μέσω ασφαλούς διαύλου επικοινωνίας . Εάν κάποιος πελάτης σκοπεύει όχι μόνο να αποθηκεύσει, αλλά και να επεξεργαστεί περαιτέρω τα δεδομένα προσωπικού χαρακτήρα εντός του υπολογιστικού νέφους (π.χ., αναζήτηση καταχωρίσεων σε βάσεις δεδομένων), πρέπει να έχει υπόψη του ότι η κρυπτογράφηση δεν μπορεί να διατηρηθεί κατά τη διάρκεια της επεξεργασίας των δεδομένων (με εξαίρεση περιπτώσεις πολύ ειδικών υπολογισμών) – βλ. Ομάδα Εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική , της 1ης Ιουλίου 2012, σελ 20, διαθέσιμη στην ηλεκτρονική δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

144 βλ. Bob Duncan, άρθρο : "*Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing"* , CLOUD COMPUTIND 2018, The Ninth International Conference on Cloud Compyting GRIDs, and Virtualization, σελ 1.

Μάλιστα, επειδή οι χρήστες επικοινωνούν ίσως και απευθείας με τον πάροχο cloud – όταν αυτός είναι εκτελών την επεξεργασία – πρέπει ο πάροχος να προβλέψει διαδικασίες διευκόλυνσης και έγγραφα άσκησης των δικαιωμάτων των υποκειμένων.

Το privacy by default σημαίνει ότι οι προσωπικές ρυθμίσεις του χρήστη θα πρέπει να είναι εξ ορισμού ρυθμισμένες στο επίπεδο της υψηλότερης προστασίας[145], ενώ τα τεχνικά και διαδικαστικά μέτρα τα ορίζει και φροντίζει ο υπεύθυνος επεξεργασίας–πελάτης της νεφοϋπολογιστικής.

Τέλος, στις συμβατικές ρήτρες, πέρα των ως άνω μέτρων, πρέπει να ορίζονται υποχρεώσεις προστασίας του απορρήτου στους υπαλλήλους των πελατών και των παρόχων υπηρεσιών νεφοϋπολογιστικής, καθώς και στους υπεργολάβους και υπαλλήλους αυτών.

❖♓☽ **Υποχρέωση γνωστοποίησης και ανακοίνωσης παραβίασης δεδομένων[146].**

Σε περίπτωση παραβίασης προσωπικών δεδομένων (data breach), ο υπεύθυνος επεξεργασίας υποχρεούται, να γνωστοποιήσει αμελλητί και, εάν είναι δυνατό, εντός 72 ωρών από τη στιγμή που λάβει γνώση του γεγονότος, την παραβίαση στην αρμόδια εποπτική αρχή, εκτός αν η παραβίαση αυτή δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων[147]. Υπό συγκεκριμένες προϋποθέσεις υποχρεούται να τη γνωστοποιήσει και στο υποκείμενο των δεδομένων , εκτός αν έχει λάβει μέτρα που καθιστούν μη κατανοητά τα δεδομένα προσωπικού χαρακτήρα σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά, όπως η κρυπτογράφηση[148] (αρ. 34 Κανονισμού 2016/679/ΕΕ).

Η γνωστοποίηση πρέπει κατ' ελάχιστο να: α) περιγράφει τη φύση της παραβίασης προσωπικών δεδομένων, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων, β) ανακοινώνει το όνομα και τα στοιχεία του υπεύθυνου προστασίας δεδομένων ή άλλου σημείου επικοινωνίας, γ) περιγράφει τις ενδεχόμενες συνέπειες της παραβίασης, δ) περιγράφει τα ληφθέντα ή προτεινόμενα προς λήψη μέτρα από

145 π.χ σε μια ιστοσελίδα ενός κοινωνικού δικτύου (εδώ και ο πάροχος υπηρεσιών νέφους μπορεί να είναι υπεύθυνος επεξεργασίας), όταν ένας χρήστης δημιουργεί έναν λογαριασμό, θα πρέπει οι ρυθμίσεις που αφορούν στο ποιός θα είναι σε θέση να δει την δραστηριότητά του να είναι by default από τον πάροχο ρυθμισμένες στο "κανένας". Ο χρήστης, δύναται ωστόσο να ορίσει ο ίδιος άλλες ρυθμίσεις και να επιτρέπει πρόσβαση π.χ. στις φωτογραφίες του μόνο σε διαδικτυακούς του φίλους που έχουν λογαριασμό στο ίδιο κοινωνικό δίκτυο.

146 Βλ. Article 29 Data Protection Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, adopted on 3 October 2017. Βλ. και *Παναγοπούλου – Κουτνατζή Φ.*, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ, σελ. 32.

147 Όταν δε η γνωστοποίηση καθυστερήσει πέραν των 72 ωρών συνοδεύεται από αιτιολόγηση για την καθυστέρηση 33 παρ. 1 Κανονισμού 2016/679 (ΕΕ)

148 Άρ 34 παρ. 3 περ. α' Κανονισμού 2016/679 (ΕΕ)

τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της[149]

Τέλος, ο εκτελών την επεξεργασία σε περίπτωσης παραβίασης, υποχρεούται να ενημερώσει αμελλητί τον υπεύθυνο επεξεργασίας για αυτήν[150].

❖♓♓◑ **Συγκατάθεση του υποκειμένου**:

Η νομιμότητα της επεξεργασίας[151], εξαρτάται από τη λήψη έγγραφης προηγούμενης, ρητής συγκατάθεσης από το υποκείμενα των δεδομένων[152]. Συγκατάθεση είναι κάθε ένδειξη βούλησης, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιδεινώσει με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν, η οποία δύναται ανά πάσα στιγμή να ανακληθεί με μελλοντική ισχύ[153].

Επίσης , ο Γενικός Κανονισμός στο άρθρο 8 για πρώτη φορά θεσπίζει ένα πιο ενισχυμένο πλαίσιο προστασίας αναφορικά με τη λήψη συγκατάθεσης από παιδιά στα πλαίσια της προσφοράς της υπηρεσίας της κοινωνίας των πληροφοριών (άρα και του cloud computing κ.ά.) όπως το κατέβασμα ενός ring tone, η εγγραφή σε κοινωνία δίκτυα, η επεξεργασία δεδομένων με σκοπό την στοχευμένη –

149 Βλ. αναλυτ. άρ. 33 παρ. 3 Κανονισμού 2016/679 (ΕΕ).

150 βλ. Άρθρο 33 παρ. 1 εδ β΄, Κανονισμού 679/2018/ΕΕ και βλ. Φερενίκη Παναγοπούλου Κούτνατζη Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 679/2016/ΕΕ, εκδόσεις Σάκκουλα 2017, σελ 35

151 Βέβαια, υπάρχουν και εξαιρέσεις όπου δεν απαιτείται η συγκατάθεση του υποκειμένου, *βλ. Άρθρο 6, παρ 1 περ β,γ,δ,ε,στ και άρθρο 9 παρ. 2 περ β,γ,δ,ε,στ,ζ,η,θ,ι Κανονισμού 2016/679 (ΕΕ)*, όπως όταν επεξεργασία διενεργείται για: 1.- την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης, 2.- τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας, 3.- τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, 4.- την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, 5.- απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί , για τις ειδικές κατηγορίες προσωπικών δεδομένων

152 βλ. Άρθρα 4 στοιχ 11 , 7, 8 και 9 Κανονισμού 2016/679 (ΕΕ)

153 Η CNIL προέβη σε ελέγχους και συστάσεις στην εταιρία Microsoft, όσον αφορά στο λογισμικό των Windows 10, καθώς μεταξύ άλλων πλημμελειών, παρατήρησε ότι η εταιρία για όποιον χρήστη κατέβαζε το εν λόγω λογισμικό, παρακολουθούσε την κίνησή του στο διαδίκτυο χωρίς τη λήψη της συγκατάθεσής του. Σε συμμόρφωση με τις ως άνω συστάσεις η Microsoft έλαβε τα εξής μέτρα : α.- οι χρήστες ενημερώνονται με σαφή και επαρκή τρόπο, ότι ένα αναγνωριστικό συσκευής - διαφήμισης προορίζεται για να παρακολουθεί την περιήγησή τους στο διαδίκτυο, προκειμένου να προσφέρει εξατομικευμένη διαφήμιση, β.- επιπλέον, η εγκατάσταση του λογισμικού, πραγματοποιείται μόνο εφόσον ο χρήστης εκφράσει ρητά την επιλογή του σχετικά με την ενεργοποίηση ή απενεργοποίηση του αναγνωριστικού διαφήμισης, γ.- μετά την εγκατάσταση, η ανάκληση/ ανατροπή του αναγνωριστικού, είναι πλέον δυνατή ανά πάσα στιγμή, βλ. περισσότερα άρθρο Windows 10: official closure of the formal notice procedure served on MICROSOFT CORPORATION *29 June 2017,* διαθέσιμο στην ηλ δ/νση : https://www.cnil.fr/en/windows-10-official-closure-formal-notice-procedure-served-microsoft-corporation,

προσωποποιημένη διαφήμιση κ.ά)[154] και απαιτεί μία ψηφιακή συναίνεση για την επεξεργασία από το παιδί, όταν αυτό είναι τουλάχιστον 16 ετών . Σε διαφορετική περίπτωση η συγκατάθεση πρέπει δίνεται από τον έχοντα τη γονική μέριμνα του παιδιού και να λαμβάνονται μέτρα για τη επαλήθευση της ταυτότητας του τελευταίου[155] .

Ο υπεύθυνος επεξεργασίας, αφού λάβει υπόψιν του τη διαθέσιμη τεχνολογία, οφείλει να προβαίνει σε όλες τις απαραίτητες ενέργειες προκειμένου να πιστοποιεί την ηλικία του χρήστη που εισέρχεται στις υπηρεσίες του (π.χ. να ζητάει ημερομηνία γέννησης) και εφόσον διαπιστώσει ότι πρόκειται για παιδί[156] ηλικίας μικρότερης των 16 ετών, θα πρέπει να διαπιστώσει ότι το πρόσωπο που συγκατατέθηκε για λογαριασμό του ανηλίκου είναι όντως ο ασκών τη γονική του μέριμνα[157].... Γίνεται άμεσα αντιληπτό πόσο δύσκολη είναι η ως άνω επαλήθευση, μέσω ενός δικτύου στο υπολογιστικό νέφος... Τη νόμιμη λήψη της συγκατάθεσης δε, οφείλει να την αποδεικνύει κιόλας (opt – in).

---

154 Ο Κανονισμός , δεν επεξηγεί τον όρο " υπηρεσίας της κοινωνίας των πληροφοριών". Ωστόσο είναι χρήσιμος ο ορισμός που δίνεται στην αιτιολογική σκέψη 18 της Οδηγίας 2000/31 για το ηλεκτρονικό εμπόριο οι υπηρεσίες της κοινωνίας της πληροφορίας καλύπτουν μεγάλο φάσμα οικονομικών δραστηριοτήτων σε απευθείας σύνδεση (on-line) οι οποίες μπορούν να συνίστανται, συγκεκριμένα, στην πώληση εμπορευμάτων σε απευθείας σύνδεση ενώ δεν καλύπτονται δραστηριότητες όπως η παράδοση αγαθών ή η παροχή υπηρεσιών off-line. Οι υπηρεσίες της κοινωνίας της πληροφορίας δεν περιορίζονται σε υπηρεσίες επιτρέπουσες τη σύναψη συμβάσεων σε απευθείας σύνδεση αλλά επίσης, εφόσον συνιστούν οικονομικές δραστηριότητες, εκτείνονται και σε υπηρεσίες που δεν αμείβονται από τον αποδέκτη τους, όπως είναι η παροχή πληροφοριών σε απευθείας σύνδεση ή εμπορικές επικοινωνίες, ή οι υπηρεσίες αναζήτησης, πρόσβασης και ανάκτησης δεδομένων. Οι υπηρεσίες της κοινωνίας της πληροφορίας καλύπτουν επίσης τη διαβίβαση πληροφοριών μέσω ενός δικτύου επικοινωνίας, με την παροχή πρόσβασης σε δίκτυο επικοινωνίας ή με την καταχώριση πληροφοριών τις οποίες παρέχει ο αποδέκτης της υπηρεσίας. Η τηλεοπτική μετάδοση κατά την έννοια της οδηγίας 89/552/ΕΚ και η ραδιοφωνική μετάδοση δεν αποτελούν υπηρεσίες της κοινωνίας της πληροφορίας διότι δεν παρέχονται κατόπιν ατομικού αιτήματος. Αντιθέτως, οι υπηρεσίες που διαβιβάζονται από σημείο σε σημείο, όπως η μαγνητοσκόπηση κατ' αίτηση ή η παροχή εμπορικών επικοινωνιών μέσω ηλεκτρονικού ταχυδρομείου, αποτελούν υπηρεσίες της κοινωνίας της πληροφορίας. Η χρήση ηλεκτρονικού ταχυδρομείου ή αντίστοιχων ατομικών επικοινωνιών, π.χ., από φυσικά πρόσωπα που δεν ενεργούν στο πλαίσιο της εμπορικής ή επαγγελματικής τους δραστηριότητας, συμπεριλαμβανομένης της χρήσης τους προς σύναψη συμβάσεων μεταξύ των εν λόγω προσώπων, δεν αποτελεί υπηρεσία της κοινωνίας της πληροφορίας. Η συμβατική σχέση μεταξύ εργαζομένου και εργοδότη δεν αποτελεί υπηρεσία της κοινωνίας της πληροφορίας. Οι υπηρεσίες οι οποίες εξ ορισμού δεν παρέχονται εξ αποστάσεως και με ηλεκτρονικά μέσα, όπως ο κατά νόμον έλεγχος των λογιστικών εταιρείας ή η παροχή ιατρικών συμβουλών όταν απαιτείται φυσική εξέταση του ασθενούς, δεν αποτελούν υπηρεσίες της κοινωνίας της πληροφορίας, διαθέσιμη στην ηλ δ/νση:
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EL:HTML
Για παράδειγμα , δεν εμπίπτει στο προστατευτικό πεδίο υπηρεσιών κοινωνίας πληροφορίας υπηρεσίες που έλαβαν μέρος μη διαδικτυακώς αλλά πραγματώνονται διαδικτυακά π.χ. Διαφήμιση μέσω ηλεκτρονικού μηνύματος σε μαθητές, οι οποίοι προηγουμένως είχαν γράψει τη δ/νση τους σε ένα κουπόνι παραγγελίας σε ένα νεανικό περιοδικό - *Φερενίκη Παναγοπούλου – Κουντατζή Φ.*, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ, σελ. 48 επ.

155 Βλ *Αλεξανδροπούλου – Αιγυπτιάδου Ευγενία*, Η προστασία των προσωπικών δεδομένων ανηλίκων στον Γενικό Κανονισμό Προστασίας Δεδομένων 2016/679 ,ΔΙΜΕΕ 1/2018

156 Βλ αιτιολογική σκέψη 38: Τα παιδιά αποτελούν μια ευάλωτη ομάδα φυσικών προσώπων καθώς χαρακτηρίζονται από επιπολαιότητα και πνευματική ανωριμότητα όσον αφορά στους κινδύνους και την προστασία των δικαιωμάτων τους και επομένως χρήζουν αυξημένης προστασίας.

157 Θα πρέπει π.χ πρώτα να ερωτάται η ηλικία του υποκειμένου και αν αυτή είναι μικρότερη των 16 ετών, τότε να ζητάται η λήψη της συγκατάθεσης από τον ασκούντα τη γονική μέριμνα. Για την επιβεβαίωση ωστόσο του προσώπου, θα πρέπει να αποστέλλεται ένα επιβεβαιωτικό μήνυμα στο e-mail του ασκούντα τη γονική μέριμνα .

❖♓♓♓◑ **ορισμός Υπεύθυνου Προστασίας Δεδομένων (Data Protection Officer– DPO)**[158].

Ο υπεύθυνος επεξεργασίας ορίζει υπεύθυνο προστασίας δεδομένων (Data Protection Officer) στις προβλεπόμενες από το άρθρο 37 του Κανονισμού περιπτώσεις και επίσης, δημοσιεύει τα στοιχεία επικοινωνίας του τελευταίου και τα ανακοινώνει στην εποπτική αρχή.

3.7 Διαβιβάσεις δεδομένων εκτός Ε.Ε

Σύμφωνα με τον Κανονισμό 2016/679 (ΕΕ), καταρχάς, η "ευθύνη" και απόφαση για τη διαβίβαση, βαρύνει τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία, οι οποίοι χρησιμοποιούν διάφορους μηχανισμούς που εγγυώνται την ασφαλή διαβίβαση[159] όπως οι "αποφάσεις επάρκειας" της Ευρωπαϊκής Επιτροπής[160].

Ελλείψει απόφασης επάρκειας, η διαβίβαση μπορεί να γίνει εφόσον ο υπεύθυνος επεξεργασίας ή ο εκτελών αυτή έχει παράσχει κατάλληλες εγγυήσεις σε συνδυασμό με την προϋπόθεση, ότι τα υποκείμενα των δεδομένων έχουν εκτελεστά δικαιώματα και αποτελεσματικά ένδικα μέσα, όπως είναι οι εταιρικοί δεσμευτικοί κανόνες (στην περίπτωση ομίλου επιχειρήσεων ή ομίλου εταιρειών που ασκούν κοινή οικονομική δραστηριότητα), οι τυποποιημένες συμβατικές ρήτρες που έχουν λάβει την έγκριση της Ευρωπαϊκής Επιτροπής ή η τήρηση ενός κώδικα δεοντολογίας ή μηχανισμού πιστοποίησης παράλληλα με την εφαρμογή κατάλληλων εγγυήσεων για τα δικαιώματα των υποκειμένων.

158 Για τον ορισμό, τη θέση και τα καθήκοντα του υπεύθυνου προστασίας δεδομένων βλ. άρ. 37, 38 και 39 Κανονισμού, καθώς και Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), adopted on 13 December 2016,, διαθέσιμη στην ηλεκτρονική δ/νση https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf. Βλ. και *Παναγοπούλου – Κουτνατζή Φ.*, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων 679/2016/ΕΕ, σελ. 34, Βλ επίσης *Βασίλης Σωτηρόπουλος*, Υπεύθυνος Προστασίας Δεδομένων, εργαλειοθήκη για το νέο θεσμό σε δημόσιο και ιδιωτικό φορέα, εκδόσεις Σάκκουλα 2017 .

159 βλ. Άρθρα 44 επ Κανονισμός 2016/679 (ΕΕ) και https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_el

160 Μία τρίτη χώρα, μπορεί να ζητήσει μέσω απόφασης επάρκειας της Ευρωπαϊκής Επιτροπής να κηρυχθεί ως προσφέρουσα επαρκές επίπεδο προστασίας. Σε αυτή την περίπτωση η διαβίβαση των δεδομένων στην τρίτη αυτή χώρα εξομοιώνεται με διαβίβαση δεδομένων εντός Ε.Ε./ βλ. Άρθρο 45 Κανονισμού 2016/679 (ΕΕ). Ωστόσο στην υπόθεση Schrems, το Ευρωπαϊκό Δικαστήριο ακύρωσε την απόφαση επάρκειας του "ασφαλούς λιμένα" (Safe Harbor), μεταξύ Ευρώπης και ΗΠΑ, καθώς διαπίστωσε ότι πρόσβαση των αμερικανικών υπηρεσιών πληροφορίας, στα δεδομένα που διαβιβάστηκαν, παραβιάζει κατάφωρα το δικαίωμα σεβασμού της ιδιωτικής ζωής και προστασίας των προσωπικών δεδομένων των Ευρωπαίων πολιτών, // βλ περισσότερα στην ηλ δ/νση https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN

Τέλος, στις εξαιρετικές περιπτώσεις που εκλείπει και απόφαση επάρκειας δυνάμει του άρθρου 45 παρ. 3 και οι κατάλληλες εγγυήσεις του άρθρου 46, συμπεριλαμβανομένων των εταιρικών δεσμευτικών κανόνων και ελλείψει αυτών, οι ειδικές προϋποθέσεις του άρθρο 49 παρ. 2, η διαβίβαση δεδομένων σε τρίτη χώρα θα πραγματοποιηθεί μόνον εάν η διαβίβαση δεν είναι επαναλαμβανόμενη, αφορά μόνο περιορισμένο αριθμό υποκειμένων των δεδομένων, είναι απαραίτητη για τους σκοπούς επιτακτικών έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας των οποίων δεν υπερισχύουν τα συμφέροντα ή τα δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων και ο υπεύθυνος επεξεργασίας έχει εκτιμήσει όλες τις περιστάσεις που σχετίζονται με τη διαβίβαση των δεδομένων και έχει παράσχει, βάσει της εν λόγω εκτίμησης, τις δέουσες εγγυήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα, με υποχρέωσή του να ενημερώσει σχετικά την εποπτική αρχή και το υποκείμενο για τη διαβίβαση[161].

3.8 Ευθύνη υπεύθυνου επεξεργασίας και εκτελούντος την επεξεργασία.

Σε περίπτωση που το υποκείμενο υπέστη ζημία (υλική ή μη) ως αποτέλεσμα παραβίασης του Κανονισμού, δικαιούται αποζημίωσης από τον υπεύθυνο ή τον εκτελούντα την επεξεργασία, οι οποίοι ευθύνονται αλληλεγγύως και εις ολόκληρον.

Εάν περισσότεροι του ενός υπεύθυνοι επεξεργασίας ή εκτελούντες την επεξεργασία ή αμφότεροι ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία εμπλέκονται στην ίδια επεξεργασία και, εάν δυνάμει των παραγράφων 2 και 3 του άρθρου 82, είναι υπεύθυνοι για τυχόν ζημία που προκάλεσε η επεξεργασία, κάθε υπεύθυνος επεξεργασίας ή εκτελών την επεξεργασία ευθύνεται για τη συνολική ζημία, προκειμένου να διασφαλιστεί αποτελεσματική αποζημίωση του υποκειμένου των δεδομένων.

Ο Νέος Κανονισμός 2016/679 (ΕΕ) σε αντίθεση με την προηγούμενη Οδηγία 95/46 ΕΚ, ενισχύει τις υποχρεώσεις του εκτελούντα την επεξεργασία και ορίζει για πρώτη φορά δική του ξεχωριστή ευθύνη[162], σε περίπτωση μη συμμόρφωσής του με τις υποχρεώσεις που ορίζει ο Κανονισμός ή αντίθετης ενέργειας ή καθ' υπέρβαση των νομίμων εντολών που έλαβε από τον υπεύθυνο επεξεργασίας.

3.9 Κυρώσεις

161 Βλ. αναλυτ. άρ. 49 Κανονισμού.
162 βλ. Άρθρο 82 Κανονισμού 2016/679 ΕΕ

Ο Γενικός Κανονισμός εισάγει ενιαίες για ολόκληρο τον ευρωπαϊκό χώρο αυστηρότατες διοικητικές κυρώσεις για τους υπεύθυνους επεξεργασίας στις περιπτώσεις παραβίασης των διατάξεών του[163]. Παρέχει μια εναρμονισμένη προσέγγιση για τις παραβιάσεις από τους υπεύθυνους επεξεργασίας και των εκτελούντων αυτήν, των υποχρεώσεων που απαριθμούνται ρητά στις παραγράφους 4 μέχρι και 6 του άρθρου 83. Τα διοικητικά πρόστιμα, επιβάλλονται για μία μεγάλη ποικιλία παραβάσεων και δύνανται να φθάσουν μέχρι 20.000.000,00 EUR ή, σε περίπτωση επιχειρήσεων, έως το 4 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο[164]!

3.10 Ο πάροχος υπηρεσιών υπολογιστικής νέφους ως εκτελών την επεξεργασία - Ο πελάτης υπηρεσιών υπολογιστικής νέφους ως υπεύθυνος επεξεργασίας .

3.10.1 Ο πάροχος υπηρεσιών υπολογιστικής νέφους ως εκτελών την επεξεργασία.

Όπως ήδη προεκτέθηκε, ο Κανονισμός 2016/679/ΕΕ, ενισχύει τις υποχρεώσεις και θεσπίζει άμεση ευθύνη του εκτελούντα την επεξεργασία, ο οποίος πρέπει να συμμορφώνεται με τις διατάξεις του. Επομένως και του παρόχου υπηρεσιών cloud, που καλείται πλέον να συμμορφωθεί με τις νέες υποχρεώσεις, μεταξύ των οποίων η επαρκής τεκμηρίωση (έγγραφη) για όλες τις δραστηριότητες επεξεργασίας δεδομένων, η λήψη κατάλληλων προτύπων ασφαλείας, οι τακτικοί έλεγχοι προστασίας των δεδομένων, η αξιολόγηση των επιπτώσεων, ο διορισμός υπεύθυνου προστασίας, η συνεργασία με την αρμόδια αρχή προστασίας δεδομένων κ.ά.

Προκύπτει λοιπόν το ερώτημα κατά πόσο είναι δυνατόν να εφαρμοστεί ο Κανονισμός 2016/679 (ΕΕ), στις ήδη υπάρχουσες ολοκληρωμένες τεχνικά και υπηρεσιακά δομές του υπολογιστικού νέφους που βρίσκονται σε όλο τον κόσμο, όπου εμπλέκονται πολλά μέρη με διαφορετικούς ρόλους ή/και εναλλαγή αυτών, η ευθύνη μετακυλίεται από το ένα μέρος στο άλλο και η επεξεργασία εναλλάσσεται διαρκώς .

163 Βλ. Article 29 Data Protection Working Party, Guidelines on the application and setting administrative fines for the purposes of the Regulation 2016/697, adopted on 3 October 2017, διαθέσιμη στην ηλεκτρονική δ/νση : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611237

164 Βλ περισσότερα *Κομνηνός Γ. Κόμνιος*, Οι γενικοί όροι επιβολής διοικητικών προστίμων κατά τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, Συμβολή στην ερμηνεία του άρθρου 83 του γενικού Κανονισμού για την Προστασία των Δεδομένων, ΔΙΜΕΕ τ. 4/2017

Οι πάροχοι, διαθέτουν εγκαταστάσεις σε διάφορες χώρες ανά τον κόσμο και εξυπηρετούν εκατομμύρια πελάτες, η δε πλειοψηφία τους εδρεύει εκτός ευρωπαϊκής ένωσης. Μέχρι σήμερα οι πελάτες τους – υπεύθυνοι επεξεργασίας, απλά συμφωνούσαν με τους ήδη προδιατυπωμένους όρους των CSPs και μάλιστα με ειδικότερες ρήτρες που τους υπήγαγαν ίσως και στο δίκαιο μιας άλλης χώρας (εκτός Ε.Ε.), χωρίς να έχουν τη δυνατότητα διαπραγμάτευσης οποιουδήποτε όρου[165]. Επίσης, οι πλατφόρμες, η δομή και ο τρόπος παροχής των υπηρεσιών τους είναι προσχεδιασμένα, και φυσικά δυσκίνητα ως προς την όποια αλλαγή.

Διερωτάται κανείς λοιπόν, πώς είναι δυνατόν, ο πελάτης παροχής υπηρεσιών, ως υπεύθυνος επεξεργασίας, να μπορεί να δώσει τις “καταγεγραμμένες” εντολές, σύμφωνα με το άρθρο 28 του Κανονισμού και οι πάροχοι να τις ακολουθήσουν[166], τη στιγμή που οι τελευταίοι, επιθυμούν να διατηρήσουν την ευελιξία τους στην όποια επεξεργασία ή παρεχόμενη υπηρεσία τους.

Το άρθρο 28 παραθέτει μία λίστα με υποχρεωτικούς συμβατικούς όρους μεταξύ του υπεύθυνου επεξεργασίας και του εκτελούντος αυτήν, που περιέχονται σε έγγραφη σύμβαση. Στη σύμβαση αυτή θα καθορίζεται εγγράφως, το αντικείμενο, η διάρκεια, η φύση, ο σκοπός και ο τρόπος της επεξεργασίας από τον εκτελούντα (κατ' εντολή και) για λογαριασμό του υπεύθυνου επεξεργασίας, το είδος των προσωπικών δεδομένων, οι κατηγορίες των υποκειμένων και οι εν γένει υποχρεώσεις και δικαιώματα του υπεύθυνου επεξεργασίας. Επιπροσθέτως και σημαντικότερο, θα πρέπει να διαλαμβάνονται όροι, οι οποίοι να υποχρεώνουν τον εκτελούντα την επεξεργασία – ήτοι τον πάροχο – να δεσμεύει το προσωπικό του με ρήτρες εμπιστευτικότητας ώστε να διασφαλίζεται το απόρρητο, να λαμβάνει κατάλληλα μέτρα ασφαλείας για την προστασία των δεδομένων από απώλεια, καταστροφή, αλλοίωση ή μη εξουσιοδοτημένη επεξεργασία, να συμφωνεί με τον υπεύθυνο επεξεργασίας τις αναγκαίες τεχνικές και οργανωτικές απαιτήσεις για την ενίσχυση και εκπλήρωση – πραγματοποίηση των δικαιωμάτων των υποκειμένων, να βοηθάει αυτόν στην υποχρέωσή του να ειδοποιεί την αρμόδια εποπτική αρχή σε περίπτωση παραβίασης των δεδομένων και φυσικά να επιστρέφει όλα τα προσωπικά δεδομένα μετά το πέρας της επεξεργασίας ή τον τερματισμό της σύμβασης παροχής υπηρεσιών στον υπεύθυνο επεξεργασίας.

---

165 Βλ Mark Webber, Partner with Fieldfisher (Silicon Valley), examines the impact of the new General Data Protection Regulation on cloud service providers , άρθρο “The GDPR's impact on the cloud computing service provider as a processor”, / Privacy & Data Protection, VOLUME 16, ISSUE 4, διαθέσιμο και στην ηλ δ/νση https://www.fieldfisher.com/media/3993765/the-gdprs-impact-on-the-cloud-service-provider-as-a-processor-mark-webber-privacy-data-protection.pdf

166 βλ. Ευγενία Σμυρνάκη, Υπ. Διδάκτωρ Νομικής Σχολής ΑΠΘ, Υπολογιστικό Νέφος (Cloud) και Προσωπικά Δεδομένα - Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016 , διαθέσιμη στην ηλ δ/νση : http://epublications.web.auth.gr/sites/default/files/%CE%A3%CE%BC%CF%85%CF%81%CE%BD%CE%AC%CE%BA%CE%B7%20%CE%A5%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%B9%CE%BA%CF%8C%20%CE%9D%CE%AD%CF%86%CE%BF%CF%82.pdf

Επομένως, ένα θέμα που προκύπτει, αφορά στη σύμβαση μεταξύ παρόχου και πελάτη, ήτοι υπεύθυνου επεξεργασίας και εκτελούντος αυτήν.

Επιπροσθέτως, σύμφωνα με το άρθρο 28 παρ. 2, ο εκτελών την επεξεργασία - CSP, υποχρεούται να ενημερώνει εγγράφως τον υπεύθυνο επεξεργασίας, τον πελάτη δηλαδή, για την πρόσληψη έτερου υποεκτελούντος την επεξεργασία – υπεργολάβου[167]. Αφής ωστόσο, οι υπηρεσίες του CSP παρέχονται με αυτοματοποιημένα μέσα και διαδικασίες, βασισμένες σε προδιατυπωμένους όρους, πώς θα ενημερώνεται ο κάθε πελάτης ξεχωριστά από τον τελικό πάροχο σχετικά με την πρόσληψη άλλου υποεκτελούντος; Αλλά ακόμη και αν ενημερωθεί, τι γίνεται στην περίπτωση που ο πελάτης δεν συμφωνεί με αυτή;

Φυσικά, προϋπόθεση της συνεργασίας ενός παρόχου με κάποιον υποεκτελούντα την επεξεργασία, αποτελεί η συμμόρφωση του τελευταίου στον Κανονισμό. Ο κάθε δε υποεκτελών αναλαμβάνει συγκεκριμένες δραστηριότητες επεξεργασίας που του αναθέτει ο πάροχος αναφορικά με τον κάθε πελάτη χωριστά και στην περίπτωση που αποτύχει να εκπληρώσει τις υποχρεώσεις αυτές, ο πάροχος παραμένει πλήρως υπεύθυνος έναντι του πελάτη για τις πράξεις του υπεργολάβου του. Επομένως, στη μεταξύ τους σύμβαση (παρόχου – υπεργολάβου) θα πρέπει να διαλαμβάνονται οι ίδιοι όροι που έχουν συμφωνηθεί και στη σύμβαση μεταξύ παρόχου και του συγκεκριμένου πελάτη! Γίνεται αντιληπτό πώς κάτι τέτοιο είναι σχεδόν ανέφικτο να πραγματοποιηθεί στο cloud[168].

Όλα τα ανωτέρω, θεσπίζουν πρόσθετες υποχρεώσεις για τους παρόχους υπηρεσιών cloud. Παράλληλα όμως υποχρεώνουν τον πελάτη, να δοκιμάσει και να εξετάσει διεξοδικά τη “λύση” - υπηρεσία υπολογιστικού νέφους που αγοράζει..

Ο Κανονισμός 2016/679 (ΕΕ) θεσπίζει πρόσθετη υποχρέωση αυτή, της τήρησης αρχείου επεξεργασίας δραστηριοτήτων και για τον υπεύθυνο επεξεργασίας και για τον εκτελούντα αυτήν. Επιπροσθέτως η αρμόδια εποπτική αρχή, δύναται πλέον να ζητήσει απευθείας από τον εκτελούντα την επεξεργασία οποιαδήποτε

---

167 Αρκεί και μία προκαταβολική γενική συναίνεση του πελάτη, που θα επιτρέπει στον πάροχο την πρόσληψη άλλων υπεργολάβων – υποεκτελούντων την επεξεργασία. Ωστόσο αυτή δεν αίρει την υποχρέωση του CSP για ενημέρωση του υπεύθυνου επεξεργασίας σχετικά με αλλαγές στις διαδικασίες και τους υπεργολάβους του.

168 βλ ενδεικτικά, πρόσθετη πράξη για την επεξεργασία δεδομένων της εταιρίας υπηρεσιών νέφους IBM, η οποία, ενώ έχει καταρτισθεί (με προδιατυπωμένους πάλι όρους από την IBM) σε συμμόρφωση με τον Κανονισμό 2016/679 (ΕΕ), στον όρο 7 “υπεργολάβοι που εκτελούν επεξεργασία”, παρ. 7.1 αναφέρει “.... ***Η IBM θα επιβάλει ουσιωδώς παρόμοιες υποχρεώσεις προστασίας δεδομένων*** *με εκείνες που ορίζονται στην παρούσα Πρόσθετη Πράξη DPA* ***σε οποιονδήποτε εγκεκριμένο Υπεργολάβο*** *που εκτελεί επεξεργασία προτού ο Υπεργολάβος προβεί στην Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα του πελάτη...*” και στην παρ . 7.2 “.... ***Εάν ο Πελάτης*** *υποβάλει δικαιολογημένα* ***ένσταση*** *κατά της προσθήκης ενός Υπεργολάβου που Εκτελεί Επεξεργασία* ***και η IBM δεν μπορεί να ανταποκριθεί εύλογα*** *στην ένσταση του Πελάτη, η IBM θα ειδοποιήσει τον Πελάτη σχετικά.* ***Ο Πελάτης μπορεί να διακόψει τις αντίστοιχες Υπηρεσίες*** .....”, διαθέσιμη στην ηλ δ/νση https://www.ibm.com/support/customer/pdf/dpa_el.pdf . Ποιος καθορίζει και πώς ελέγχει τις “*ουσιωδώς παρόμοιες υποχρεώσεις*” του υπό εκτελούντος την επεξεργασία και τι επιβαρύνσεις συνεπάγεται η διακοπή της συνεργασίας με τον συγκεκριμένο πάροχο για τον πελάτη που εναντιώνεται ;

πληροφορία, στα πλαίσια της άσκησης των καθηκόντων της. Επίσης, ορίζεται ότι ο υπεύθυνος επεξεργασίας και ο εκτελών, διορίζουν υπεύθυνο προστασίας δεδομένων προσωπικού χαρακτήρα ιδίως στις περιπτώσεις που οι δραστηριότητες της επεξεργασίας συνιστούν πράξεις μεγάλης κλίμακας ειδικών κατηγοριών δεδομένων ή απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων σε μεγάλη κλίμακα. Τα ανωτέρω, απαιτούν σημαντικές οικονομικές επενδύσεις από τους παρόχους – εκτελούντες την επεξεργασία.

Παρόλο που ο υπεύθυνος επεξεργασίας ορίζει τα τεχνικά και οργανωτικά μέτρα για την προστασία και ασφάλεια των δεδομένων, πρακτικά, ο πάροχος είναι αυτός που επιφορτίζεται ειδικά με την λήψη των τεχνικών μέτρων ασφαλείας π.χ ψευδωνυμοποίηση, κρυπτογράφηση, μέτρα που εξασφαλίζουν την ακεραιότητα και τη διαθεσιμότητα των δεδομένων αν προκύψει κάποιο περιστατικό. Ο πελάτης περιορίζεται κατά κύριο λόγο στο να εξακριβώσει αν αυτά είναι ικανά, ενδεδειγμένα και αποτελεσματικά, κάτι δε που προϋποθέτει ικανές γνώσεις της Τ.Π. Οι τακτικοί έλεγχοι για την αποτελεσματικότητά τους πρέπει να διενεργούνται και πάλι από τους παρόχους, αφού η ευθύνη πλέει ανάμεσα στον υπεύθυνο επεξεργασίας και το εκτελούντα αυτή.

Ωστόσο, η ως άνω υποχρέωση δημιουργεί δυσκολίες στους CSPs , ειδικά στα πλαίσια παροχής υπηρεσιών υποδομής και πλατφόρμας (IaaS και Paas). Λαμβάνοντας υπόψιν τον ευρύτατο ορισμό για τα προσωπικά δεδομένα, όπως προεκτέθηκε, και του νέου ρόλου και υποχρεώσεων του εκτελούντος την επεξεργασία, οι πάροχοι IaaS και Paas, καταρχάς πρέπει να συμμορφωθούν με το νέο νομικό πλαίσιο. Ωστόσο, σε αυτές τις υπηρεσίες οι πάροχοι περιορίζονται μόνο στην παροχή της πλατφόρμας και των πόρων Τ.Π και αγνοούν – ίσως και πλήρως – τα δεδομένα που αποθηκεύουν και επεξεργάζονται οι χρήστες – πελάτες – υπεύθυνοι επεξεργασίας, ενώ μπορεί να μην έχουν καν δυνατότητα πρόσβασης σε αυτά[169], τα οποία μπορεί να έχουν ήδη κρυπτογραφηθεί από τον πελάτη πριν την αποστολή τους στο cloud. Ο πελάτης είναι αυτός που θα λάβει τα κατάλληλα τεχνικά (π.χ κρυπτογράφηση κ.ά) και οργανωτικά μέτρα για την προστασία τους. Όμως, ως εκτελούντες την επεξεργασία οι πάροχοι, υποχρεούνται και αυτοί σε συμμόρφωση και έχουν δική τους χωριστή ευθύνη. Πώς θα είναι σε θέση, αφού αγνοούν τη φύση των δεδομένων, να επέμβουν και να λάβουν τυχόν πρόσθετα απαιτούμενα μέτρα ασφαλείας στην περίπτωση που δεν αρκούν αυτά που έχει εφαρμόσει ο πελάτης;

169 Το IaaS , δεν σχεδιάστηκε για να επεξεργάζεται προσωπικά δεδομένα. Επομένως, τα ήδη κρυπτογραφημένα από τον χρήστη δεδομένα που αυτός έχει δημιουργήσει και μεταφέρει σε δεύτερο χρόνο και σε αυτή τη μορφή στο περιβάλλον του IaaS νέφους, εμπίπτουν στην έννοια των προσωπικών δεδομένων που ορίζει ο Κανονισμός ή όχι; / βλ. περισσότερα *Massino Maggiore* , άρθρο “EU, Cloud Computing: obligations under the Directive v. GDPR”, June 2016, διαθέσιμο στην ηλ δ/νση http://www.mmlex.it/wp-content/uploads/2016/09/DPLP-June-2016-Cloud-Computing.pdf

Πρακτικά, το ανωτέρω σημαίνει ότι οι πάροχοι cloud, θα πρέπει να προσφέρουν την ασφάλεια στο νέφος, ως υπηρεσία[170] και να διεξάγουν συστηματικούς και συνεχείς ελέγχους ασφαλείας, καθώς τα συστήματα των ΤΠ εξελίσσονται συνεχώς (π.χ το λογισμικό ενημερώνεται καθημερινά, οπότε ένας ετήσιος έλεγχος κρίνεται ανεπαρκής)[171].

Μία εκ των σημαντικότερων υποχρεώσεων επίσης για αμφότερους υπεύθυνο και εκτελούντα την επεξεργασία είναι ο σεβασμός και η διευκόλυνση άσκησης[172] των δικαιωμάτων των υποκειμένων. Στα πλαίσια αυτής της υποχρέωσης, ο υπεύθυνος επεξεργασίας – πελάτης, οφείλει να εξακριβώσει ότι ο πάροχος δεν παρεμποδίζει με οποιονδήποτε τρόπο σε τεχνικό και οργανωτικό επίπεδο την άσκηση των δικαιωμάτων του υποκειμένου, ακόμη και στις περιπτώσεις στις οποίες τα δεδομένα υφίστανται μεταγενέστερη επεξεργασία από υπεργολάβους. Έτσι, π.χ, ο πάροχος ως προς το δικαίωμα πρόσβασης του υποκειμένου, θα πρέπει να διασφαλίζει με τεχνικά μέτρα τη διατήρηση της ακεραιότητας του περιεχομένου της βάσης δεδομένων όπου αυτά είναι αποθηκευμένα' θα πρέπει επιπροσθέτως να έχει λάβει και τα απαραίτητα μέτρα για να γνωρίζει την προέλευσή τους και τη διαδρομή τους[173].

Επίσης είναι ανάγκη να αναπτυχθούν και υιοθετηθούν από τους παρόχους διαλειτουργικά μοντέλα διεπαφών υπηρεσιών μεταξύ τους ικανά να ανταποκρίνονται στο δικαίωμα στη φορητότητα των υποκειμένων κ.ά. Ωστόσο, είναι αυτό εφικτό στο cloud computing και τι επιβάρυνση συνεπάγεται για τους παρόχους;

Επιπροσθέτως, ρητά πλέον ενισχύεται το δικαίωμα στη λήθη[174] που επιτάσσει τη λήψη εύλογων μέτρων, με βάση τη διαθέσιμη τεχνολογία, για τη χωρίς καθυστέρηση υλοποίηση της διαγραφής. Αν συνυπολογίσουμε όμως τη μαζική μεταφορά/ αποθήκευση δεδομένων στο cloud, το γεγονός ότι δύσκολα μπορεί να προσδιοριστεί η ακριβής τους τοποθεσία και τα χαρακτηριστικά της πολυμίσθωσης και του διαμοιρασμού των πόρων του, διερωτάται εύλογα κανείς, πώς θα βρεθεί ο αρχικός εκτελών την επεξεργασία, πώς δύναται να εντοπίσει άμεσα[175] όλους τους

170 *Ndubuisi Anomelechi, William Cooper, Bob Duncan, John D. Lamb*, άρθρο "A Management View of Security and Cloud Computing", CLOUD COMPUTING 2018 : The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, σελ 27

171 Βλ *ENISA*, Critical Cloud Computing , A CIIP perspective on cloud computing services Version 1,0, December 2012 , σελ 31, διαθέσιμο στην ηλεκτρονική δ/νση : https://www.enisa.europa.eu/publications/critical-cloud-computing

172 Βλ και αιτιολογική σκέψη 59, σύμφωνα με την οποία , ο πάροχος, σε συνεργασία με τον υπεύθυνο επεξεργασία – πελάτη, θα πρέπει να παρέχει τα μέσα για ηλεκτρονική υποβολή αιτημάτων των υποκειμένων, όταν τα δεδομένων υφίστανται ηλεκτρονική επεξεργασία.

173 Βλ. Ομάδα Εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 5/2012 σχετικά με τη νεφοϋπολογιστική της 1ης Ιουλίου 2012, , σελ 21, διαθέσιμη στην ηλεκτρονική δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

174 Βλ αναλυτικά άρθρο 17 Κανονισμού 2016/679 (ΕΕ) και αιτιολογική σκέψη 66

175 Η διαγραφή θα πρέπει να πραγματοποιηθεί εντός ενός μήνα από την υποβολή του αιτήματος του υποκειμένου. Σε κάθε δε περίπτωση όχι πλέον των δύο μηνών, διαφορετικά η καθυστέρηση της διαγραφής, θα πρέπει να αιτιολογείται. Μάλιστα η CNIL, αναφέρει ότι ένας χρήστης του διαδικτύου ηλικίας κάτω των 18 ετών, που έχει δημιουργήσει έναν ηλεκτρονικό λογαριασμό, μπορεί

άλλους υπό-εκτελούντες αυτήν, ώστε να τους ειδοποιήσει και να πράξουν τη διαγραφή; Και μάλιστα με τέτοιο τρόπο που να μην επηρεαστεί η ακεραιότητα και η διαθεσιμότητα άλλων δεδομένων που μοιράζονται τους ίδιους πόρους ΤΠ και εξαλείφοντας πλήρως οποιοδήποτε “υπόλειμμα” ικανό να επιφέρει την ανάκτηση των δεδομένων που διαγράφηκαν; Τέλος, η διαγραφή δεν πραγματοποιείται, πλην άλλων περιπτώσεων, στο βαθμό που η επεξεργασία είναι απαραίτητη για την άσκηση του δικαιώματος ελευθερίας της έκφρασης ή στην ενημέρωση[176]. Επομένως οι πάροχοι που θα δεχθούν ένα αίτημα διαγραφής θα κληθούν να αποφασίσουν ποιο δικαίωμα υπερισχύει. Ωστόσο, κανένας δεν θα διακινδυνέψει την επιβολή ενός υπέρογκου διοικητικού προστίμου στην περίπτωση μιας λανθασμένης κρίσης. Κατά συνέπεια, ελλοχεύει ο κίνδυνος της άκριτης ικανοποίησης της πλειοψηφίας των αιτημάτων διαγραφής εις βάρος των ανωτέρω δικαιωμάτων αλλά και των άλλων δεδομένων που μοιράζονται τους ίδιους πόρους ΤΠ !

Το περιβάλλον του νέφους είναι πολυεπίπεδο, με διάφορες δομές και εμπλεκόμενους φορείς, οι οποίοι δεν είναι κοινοί για κάθε πελάτη. Ακόμη και ο ίδιος ο πάροχος, που έχει την ευθύνη για τους υπεργολάβους του, αδυνατεί να παρακολουθήσει σε πραγματικό χρόνο τις αυτοματοποιημένες διαδικασίες που πραγματοποιούνται ως προς τον καθένα πελάτη. Επίσης, κανένα σύστημα δεν είναι πλήρως ασφαλές. Λειτουργικά συστήματα, πρωτόκολλα μεταφοράς, εφαρμογές λογισμικού, έχουν μεν εξελιχθεί μέχρι σήμερα αλλά με γνώμονα τη λειτουργικότητα και όχι την πλήρη ασφάλεια των δεδομένων και της ιδιωτικής ζωής[177]. Ωστόσο, το άρθρο 33 του Κανονισμού, υποχρεώνει , σε περίπτωση παραβίασης των δεδομένων, τον εκτελούντα την επεξεργασία να ενημερώνει αμελλητί τον πάροχο και τον υπεύθυνο επεξεργασίας να ενημερώνει την αρχή εντός 72 ωρών και μάλιστα σχετικά με το ποια αρχεία έχουν παραβιαστεί, αλλοιωθεί, διαγραφεί κλπ, άλλως επιβάλλεται πρόστιμο .

Αν υποθέσουμε ότι κάποιος ικανός hacker, εισβάλει στο περιβάλλον του νέφους, επιτεθεί σε κάποια δεδομένα και μετά σβήσει τα ίχνη του, ο πάροχος ίσως να μην είναι σε θέση να αντιληφθεί εγκαίρως την εν λόγω επίθεση. Ακόμη όμως και σε δεύτερο χρόνο αν γίνει αντιληπτή, ίσως να μην είναι σε θέση να εξακριβώσει ποιά δεδομένα δέχθηκαν και τι είδους επίθεση, παραβιάζοντας έτσι την υποχρέωση που ορίζει το ως άνω άρθρο[178]. Επομένως, οι πάροχοι θα πρέπει να αναπτύξουν

οποτεδήποτε να ζητήσει τη διαγραφή δεδομένων του και μάλιστα χωρίς καμία αιτιολογία, ο δε πάροχος υποχρεούται να το πράξει πάραυτα./ βλ. *CNIL*, PIA, Knowledge bases, February 2018 , σελ 41, διαθέσιμη στην ηλεκτρονική δ/νση : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

176 Βλ άρθρο 17 παρ. 2 Κανονισμού 2016/679 (ΕΕ)

177 *Bob Duncan, Andreas Happe, Alfred Bratterud,* άρθρο Using Unikernels to Address the Cloud Forensic Problem and help Achieve EU GDPR Compliance, CLOUD COMPUTING 2018 : The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, σελ. 71

178 *Bob Duncan*, άρθρο Can EU General Data Protection Regulation Compliance be Achieved When

συστήματα παρακολούθησης της ροής των δεδομένων και των κινήσεων στο cloud, τα οποία θα ανιχνεύουν άμεσα τυχούσες επιθέσεις και θα παρεμποδίζουν την περαιτέρω “αλλοίωση” των δεδομένων Ως προς την ασφαλή αποθήκευσή τους δε, μόνη λύση φαντάζει η αποθήκευση των δεδομένων σε κρυπτογραφημένη μορφή off-site[179]!

Η προστασία που προσφέρει ο Κανονισμός 2016/679 (ΕΕ) συνοδεύει τα δεδομένα, ανεξάρτητα με το πού αυτά καταλήγουν, ακόμη και αν διαβιβάζονται σε χώρες εκτός Ε.Ε., με διαφορετικές νομοθετικές ρυθμίσεις για την προστασία τους. Στο χώρο του νέφους αποτελεί καθημερινότητα η παγκόσμια ροή και διαβίβαση μεγάλου όγκου δεδομένων που αποθηκεύονται σε διακομιστές σε διάφορες χώρες. Οι πάροχοι, συχνά, δεν προσφέρουν πληροφορίες σχετικά με το πού αποθηκεύονται τα δεδομένα και το από πού μπορεί να έχει πρόσβαση κάποιος υπεργολάβος τους, με αποτέλεσμα να ελλοχεύει ο κίνδυνος της ελλιπούς προστασίας τους και προσβολής του απορρήτου και των δικαιωμάτων των υποκειμένων[180]. Η πλειοψηφία των παρόχων υπηρεσιών cloud βρίσκεται εγκατεστημένη στις Η.Π.Α. Επομένως, η προστασία των δεδομένων, εκτός συνόρων της Ένωσης αποτελεί μία πρόκληση, παρόλο που ο Κανονισμός παρέχει διάφορα χρήσιμα εργαλεία στον υπεύθυνο επεξεργασίας και τον εκτελούντα αυτή για την ασφαλή τους διαβίβαση και αποθήκευση[181]. Η γεωγραφική του υπερέκταση ωστόσο, μπορεί να οδηγήσει σε μη εκτελεστότητα[182], καθώς ανακύπτει το πρόβλημα της επέμβασης στην εδαφική κυριαρχία άλλων κρατών. Επίσης προκύπτει το ζήτημα της δικαιοδοσίας των δεδομένων που αποθηκεύονται σε έναν πάροχο νέφους εγκατεστημένο εκτός ευρωπαϊκού χώρου, οπότε και ο τελευταίος ίσως αντιμετωπίσει αντικρουόμενες νομικές υποχρεώσεις με βάση το δίκαιο της χώρας στην οποία είναι εγκατεστημένος.

Using Cloud Computing, CLOUD COMPUTING 2018, The Ninth International Canference on Cloud Computing, GRIDs, and Virtualization

179 *Bob Duncan*, άρθρο a Managment view of Security and Cloud Computing, CLOUD COMPUTING 2018, The Ninth International Canference on Cloud Computing, GRIDs, and Virtualization

180 Όπως ήδη αναπτύχθηκε, ενδέχεται τα δεδομένα να αποθηκευτούν σε τρίτη χώρα, οι νόμοι της οποίας, διαφέρουν από τους νόμους της Ένωσης για την προστασία των δεδομένων ή είναι ανεπαρκείς. Έτσι υπάρχει ο κίνδυνος, οι αρχές επιβολής του νόμου της τρίτης αυτής χώρας, να είναι σε θέση να παρακάμψουν το υποκείμενο (χωρίς συνάμα να δύναται να ασκήσει τα δικαιώματά του) και να ζητήσουν από τον πάροχο που είναι εγκατεστημένος στη χώρα τους, παράνομη κατά το δίκαιο της Ένωσης, πρόσβαση σε “ευρωπαϊκά” προσωπικά δεδομένα// βλ και Π. Κίτσος - Π. Παππά, Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους, ΔΙΜΕΕ 2/2012 .

181 Αξίζει να σημειωθούν τα εξής: όπως αναπτύχθηκε στην ενότητα 3.7, ελλείψει απόφασης επάρκειας, το κενό καλύπτεται από τους δεσμευτικούς εταιρικούς κανόνες. Ωστόσο οι τελευταίοι, τελούν υπό την έγκριση της Αρμόδιας κατά τόπο Αρχής. Υπάρχει ο κίνδυνος λοιπόν της έγκρισης διαφορετικών δεσμευτικών εταιρικών κανόνων λόγω διαφορετικής ερμηνείας από την κατά τόπο DPA. Επίσης, σύμφωνα με το άρθρο 49, παρ 1, εδ. 2 ο, ελλείψει όλων των “μηχανισμών” που σύμφωνα με τον Κανονισμό συμβάλλουν στη νόμιμη διαβίβαση και των παρεκκλίσεων που θέτει, η διαβίβαση δύναται να πραγματοποιηθεί μόνο αν δεν είναι επαναλαμβανόμενη και αφορά περιορισμένο αριθμό υποκειμένων. Δύο παράγοντες δηλαδή, που αποκλείονται στο χώρο του cloud.

182 βλ. *Marina Škrinjar Vidović**, EU DATA PROTECTION REFORM: CHALLENGES FOR CLOUD COMPUTING, διαθέσιμο στην ηλεκτρονική δ/νση : http://www.cyelp.com/index.php/cyelp/article/view/252/157

Τέλος, ο εκτελών την επεξεργασία έχει πλέον ρητά, αλληλέγγυα και εις ολόκληρον με τον υπεύθυνο επεξεργασίας, δική του ξεχωριστή ευθύνη για το σύνολο της ζημίας που μπορεί να προκληθεί, ενώ ο τελικός ζημιωθείς χρήστης είναι αυτός που θα επιλέξει κατά ποιου θα στραφεί για αποζημίωση. Αυτό μπορεί να οδηγήσει στην άσκηση σωρείας αγωγών κατά ενός οικονομικά ισχυρού παρόχου υπηρεσιών νέφους, ο οποίος φέρει και το βάρος απόδειξης της μη ευθύνης, σύμφωνα με το άρθρο 82 παρ 3 του Κανονισμού 2016/679 (ΕΕ), παρόλο που η πλημμέλεια στην επεξεργασία μπορεί να οφείλεται σε λάθος του υπεύθυνου επεξεργασίας .

Εν κατακλείδι, η συμμόρφωση με τον Κανονισμό απαιτεί αλλαγή δομών, επιχειρηματικού μοντέλου και τρόπου παροχής των υπηρεσιών και ασφάλειας, που συνεπάγονται αυξημένες οικονομικές επενδύσεις σε πολιτικές, διαδικασίες, τεχνολογίες και εκπαίδευση προσωπικού για τους παρόχους υπηρεσιών νέφους. Θα πρέπει να υιοθετούν κοινά “πρότυπα” για το cloud από τους παρόχους, που να σχετίζονται με τη διαλειτοργικότητα[183], τη φορητότητα και την ασφάλεια των δεδομένων, άρα να υιοθετηθούν διεθνώς αποδεκτές λύσεις για τα ανωτέρω. Τέλος, απαιτεί πλήρη ενημέρωση του πελάτη ως προς όλες τις πληροφορίες που απαιτούνται, για να αξιολογηθούν σωστά τα πλεονεκτήματα και τα μειονεκτήματα που έχει η χρήση των συγκεκριμένων υπηρεσιών, με γνώμονα την ασφάλεια των δεδομένων, τη διαφάνεια και την ασφάλεια του δικαίου.

3.10.2 Ο πελάτης παροχής υπηρεσιών νέφους ως υπεύθυνος επεξεργασίας- Επιλογή αξιόπιστου παρόχου νέφους

Ο πελάτης από την άλλη, πρέπει να διευρύνει τις γνώσεις του ως προς τις Τ.Π και να συνεργαστεί με τους παρόχους για τη λήψη όλων των κατάλληλων μέτρων προκειμένου να επιτύχουν αμφότεροι τη συμμόρφωση με τον Κανονισμό. Αυτός είναι ο υπεύθυνος επεξεργασίας και άρα τελικός υπεύθυνος για την επιλογή ενός αξιόπιστου παρόχου, με επαρκείς εγγυήσεις ως προς τα μέτρα τεχνικής ασφάλειας, οργάνωσης και επεξεργασίας των δεδομένων αλλά και τήρησης των μέτρων αυτών. Ο πελάτης, δεν μπορεί να επικαλεστεί πια την ύπαρξη των standard terms και την αδυναμία διαπραγμάτευσης αυτών για να “κρύψει” την ευθύνη του πίσω από αυτά.

Για να επιτευχθεί ωστόσο αυτό, ο πάροχος – εκτελών οφείλει να ενημερώνει τον πελάτη του για όλα τα συναφή ζητήματα, απαραιτήτως για όλους τους υπεργολάβους που συμβάλλουν στην παροχή της εκάστοτε υπηρεσίας καθώς και για

183 Η διαλειτουργικότητα και η δημιουργία διεπαφών είναι αναγκαία όχι μόνο ανάμεσα στις υπηρεσίες και εφαρμογές των παρόχων, αλλά και ανάμεσα στα λειτουργικά συστήματα του υπεύθυνου επεξεργασίας και εκτελούντος την επεξεργασία, καθώς έτσι διευκολύνεται η μεταξύ τους συνεργασία και άσκηση ελέγχου. Βλ. περισσότερα ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, Adopted on 22 September 2015, διαθέσιμη στην ηλεκτρονική δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

όλες τις τοποθεσίες όπου βρίσκονται κέντρα δεδομένων στα οποία δύναται να γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα[184].

Κύριος στόχος, του πελάτη υπηρεσιών νέφους είναι η ασφάλεια των δεδομένων και αυτή σημαίνει: τήρηση των αρχών επεξεργασίας (νομιμότητας, διαφάνειας, περιορισμού του σκοπού, αναλογικότητας, ακρίβειας, καθορισμού του χρόνου διάρκειας τη επεξεργασίας, ακεραιότητας και εμπιστευτικότητας και λογοδοσίας), σεβασμός των δικαιωμάτων των υποκειμένων (με έμφαση στη φορητότητα, τη δυνατότητα παρέμβασης και τη διαγραφή που δημιουργούν προβλήματα), και διασφάλιση της διαθεσιμότητας, του απορρήτου, της ακεραιότητας και της διαφάνειας των δεδομένων.

Επομένως, κρίσιμο σημείο αποτελεί η επιλογή του παρόχου υπηρεσιών νεφοϋπολογιτικής. Για να καταλήξει κάποιος σε μία “σωστή επιλογή” δέον όπως προβεί σε μία αξιολόγηση κινδύνου (risk assessment)[185]. Αυτή, είναι μία κυκλικά διενεργούμενη διαδικασία, η οποία καταρχάς αποτιμά τις πιθανές επιπτώσεις και προκλήσεις/ κινδύνους που σχετίζονται με την χρήση των υπηρεσιών του cloud και καταλήγει στα ζητήματα ασφαλείας που αφορούν στο συγκεκριμένο περιβάλλον νέφους. Αποτελείται από τρεις δραστηριότητες, ήτοι την εκτίμηση του κινδύνου, την αντιμετώπισή του και τον έλεγχο αυτού, με στόχο τον περιορισμό των απειλών και την ενίσχυση των τακτικών μέτρων ασφαλείας[186] .

Βασική αρχή της αξιολόγησης κινδύνου είναι η διατήρηση της ασφάλειας στο νέφος. Αυτό σημαίνει ότι το πλήρες σύνολο των ελέγχων ασφαλείας μιας υπηρεσίας νέφους, πρέπει να παραμένει αναλλοίωτο και σταθερό. Η δε ευθύνη εκπλήρωσης των απαιτήσεων ασφαλείας κινείται , ανάλογα με το μοντέλο, δυναμικά μέσα στο νέφος λόγω των διάφορων εμπλεκόμενων οντοτήτων (εκτελούντες – υποεκτελούντες – υπεύθυνοι επεξεργασίας).

Προκειμένου, ο πελάτης να διεξάγει μία αξιολόγηση κινδύνου, πρέπει, αφού διευκρινίσει ποια/ τι είδους δεδομένα θα εμπιστευτεί στο cloud και σε τι είδους επεξεργασία θα υποβληθούν αυτά, καταρχάς ν' αντιληφθεί τις διάφορες απειλές που σχετίζονται αντίστοιχα με την κάθε λύση, όπως η ευρεία πρόσβαση στο δίκτυο, η τοποθεσία παραμονής των δεδομένων, η πολλαπλή μίσθωση, οι διαμοιρασμένοι

184 Ομάδα Εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική , της 1ης Ιουλίου 2012, σελ 25, διαθέσιμη στην ηλεκτρονική δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

185 Εν προκειμένω, η αναλυόμενη αξιολόγηση κινδύνου, πρέπει να διακρίνεται από αυτήν που ορίζει το άρθρο 32 του Κανονισμού 2016/679 (ΕΕ) και αφορά στα προσωπικά δεδομένα, ενώ πρακτικά μπορεί να αποτελεί τμήμα αυτής.

186 Thomas Erl, Cloud Computing Αρχές, Τεχνολογία & Αρχιτεκτονική , ΣΕΙΡΑ SERVICE TECHNOLOGY ΤΗΣ PRENTICE HALL ΑΠΌ ΤΟΝ THOMAS ERL, εκδόσεις Γκιούρδας, σελ 134, και 446 επ.

ρόλοι και αρμοδιότητες του πελάτη και του παρόχου, η μείωση του ελέγχου από τον πελάτη – καταναλωτή, η εικονικοποίηση κ.ά.[187]

Το NIST Special Publication 800-37: Guide for Applying the Risk Management Framework to federal Information Systems, παρέχει μία πειθαρχημένη και δομημένη διεργασία, που ολοκληρώνει δραστηριότητες ασφαλείας πληροφοριών και διαχείρισης κινδύνου μέσα στον κύκλο ζωής ανάπτυξης στο νέφος, που αποτελείται από έξι (6) βήματα:

Για την εκτίμηση του κινδύνου, απαιτείται μία ανάλυση του περιβάλλοντος του νέφους, ώστε να αναγνωρισθούν πιθανές τρωτότητες και ατέλειες του συστήματος. Θα πρέπει επίσης ο πελάτης, να ζητήσει από τον πάροχο στατιστικά στοιχεία και πληροφορίες για προηγούμενες επιθέσεις (επιτυχείς ή αποτυχημένες) που έγιναν στο νέφος, λαμβάνοντας υπόψιν του τα δεδομένα που τυγχάνουν επεξεργασία, αποθηκεύονται και διαδίδονται μέσα από το cloud (βήμα 1ο). Στην πορεία θα πρέπει να αναγνωρίσει τις απαιτήσεις ασφαλείας του συστήματος για τη διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας[188], επιλέγοντας και προσαρμόζοντας τους αρχικούς ελέγχους ασφαλείας του συστήματος. Παράλληλα, θα αναπτύξει μία στρατηγική συνεχούς εποπτείας ώστε να διασφαλίζει την αποδοτικότητα και αποτελεσματικότητα των ελέγχων (βήμα 2ο).

Ακολουθεί, η αντιμετώπιση - χειρισμός του κινδύνου. Αυτή, σε πρώτο επίπεδο αφορά στην επιλογή της σωστής αρχιτεκτονικής και υπηρεσίας νέφους, που ταιριάζει καλύτερα με τα αποτελέσματα της προηγούμενης φάσης (εκτίμησης του κινδύνου – βήμα 3ο) και έπεται η εκτίμηση των ελέγχων ασφαλείας που έχει υλοποιήσει – παρέχει ο πάροχος. Ίσως χρειαστούν πρόσθετοι έλεγχοι από τον πάροχο ή και από τον πελάτη (βήμα 4ο). Κάποιοι κίνδυνοι ίσως εξαλειφθούν, κάποιοι μπορεί να μετριαστούν. Ο πάροχος μπορεί να συμφωνήσει να αναλάβει την ευθύνη για αυτούς, ως τμήμα των συμβατικών του υποχρεώσεων.

Τέλος, όσον αφορά στην τρίτη δραστηριότητα – έλεγχο του κινδύνου, ο πελάτης θα πρέπει να επιλέξει – καταλήξει στον πάροχο υπηρεσιών νέφους με τον οποίο θα συνεργαστεί δίνοντας έμφαση στη μεταξύ τους SLA και τη συμφωνία

187 Ο πελάτης πρέπει να είναι σε θέση να αξιολογήσει τη διαφάνεια των φυσικών και λογικών εξαρτήσεων – παραμέτρων στο cloud , να διαχωρίσει και να καταλάβει ποιος χειρίζεται τι και ποια υπηρεσία αναλογεί σε ποιο μοντέλο νέφους. π.χ όπως προαναφέρθηκε χαρακτηριστικό του νέφους αποτελεί η πολυμίσθωση και η ανθεκτικότητα. Αυτό ακριβώς το χαρακτηριστικό την ίδια στιγμή αποτελεί και πλεονέκτημα (όταν αφορά σε επιθέσεις DOS ή υπερφόρτωση) αλλά και μειονέκτημα (ως προς την ακεραιότητα των δεδομένων ή τη δυνατότητα διαγραφής τους), αφού η διαγραφή κάποιων προσωπικών δεδομένων που είναι αποθηκευμένα στον ίδιο πόρο ΤΠ με άλλα δεδομένα, ενδεχομένως μπορεί να επηρεάσει την ακεραιότητα των υπολοίπων / περισσότερα βλ ENISA, Critical Cloud Computing, A CIIP perspective on cpoud copmuting services, Version 1,0, December 2012, σελ 29, διαθέσιμο στην ηλεκτρονική δ/νση : https://www.enisa.europa.eu/publications/critical-cloud-computing

188 Εν προκειμένω, τα χαρακτηριστικά αυτά αναφέρονται και προσδιορίζουν ένα ασφαλές περιβάλλον νέφους, όπως αναπτύχθηκαν στην ενότητα 2.6.1., και δεν πρέπει να μην συγχέονται με τα αντίστοιχα χαρακτηριστικά που αφορούν στα προσωπικά δεδομένα.

υπηρεσίας (βήμα 5ο). Σε αυτές θα πρέπει να αναφέρονται όλοι οι υπό διαπραγμάτευση όροι και να περιλαμβάνονται εγγυήσεις για την έγκαιρη λ.χ. πρόσβαση του πελάτη στα χρονολόγια ελέγχου του νέφους και σχετικές λεπτομέρειες για εποπτεία αυτών. Επιπλέον, δέον όπως ο πελάτης ζητά από τον πάροχο να παρέχει επαρκείς αποδείξεις απ' τις οποίες να προκύπτει ότι οι έλεγχοι ασφαλείας που χρησιμοποιούνται για να προστατεύουν τους πόρους Τ.Π. έχουν υλοποιηθεί σωστά. Το σημαντικότερο βήμα αυτής της δραστηριότητας, αφορά στην εποπτεία – παρακολούθηση του κινδύνου και τη διασφάλιση τήρησης όλων των όρων της SLA από τον πάροχο (βήμα 6ο), μέσω της ανασκόπησης συμβάντων, της αποτίμησης αυτών και αναγνώρισης τυχόν αναγκών προσαρμογής της ακολουθούμενης πολιτικής.[189]

Όλα τα ανωτέρω όμως, προϋποθέτουν επαρκείς και ικανές γνώσεις της Τ.Π. που η πλειοψηφία των πελατών των υπηρεσιών cloud δεν διαθέτει.

Έτσι, χρήσιμη βοήθεια στην επιλογή ενός αξιόπιστου παρόχου προσφέρει η European Union Agency for Network and Information Security (ENISA[190]), ένας ευρωπαϊκός οργανισμός που αποτελεί κέντρο εμπειρογνωμοσύνης σε θέματα Ασφάλειας των Δικτύων και Πληροφοριών .

Η CNIL, έχει εκδώσει επίσης ένα εγχειρίδιο με συστάσεις και υπενθυμίσεις για τους πελάτες – υπεύθυνους επεξεργασίας (μικρών επιχειρήσεων) που επιθυμούν να χρησιμοποιήσουν υπηρεσίες cloud, για την επιλογή ενός αξιόπιστου παρόχου[191]. Η γαλλική αρχή προστασίας προσωπικών δεδομένων, προτρέπει όποιον επιθυμεί να “εμπιστευθεί”προσωπικά δεδομένα στο νέφος, να προβεί σε μία “ανάλυση κινδύνου”. Η ανάλυση αυτή, απαιτεί ο πελάτης να καθορίσει τους δικούς του νομικούς (τοποθεσία αποθήκευσης δεδομένων, εγγυήσεις ασφάλειας και εμπιστοσύνης), πρακτικούς (διαθεσιμότητα, φορητότητα) και τεχνικούς (διαλειτουργικότητα, εγγύηση επαρκούς επιπέδου διαθεσιμότητας δικτύου) περιορισμούς και όρους και να

189 Για το σκοπό αυτό, είναι ουσιαστικής σημασίας οι πάροχοι υπηρεσιών νέφους να παρέχουν στον πελάτη , επαρκή και λεπτομερειακή πληροφόρηση σχετικά με τα μέτρα ασφαλείας που εφαρμόζει σε σχέση με τις ατέλειες και τρωτότοτητες της υπηρεσίας και της υποδομής του αλλά και τη διαχείριση των κινδύνων και αποφάσεων που ο ίδιος ο πάροχος διενεργεί και λαμβάνει αντίστοιχα. Μόνο τότε ο πελάτης θα είναι σε θέση να διενεργήσει τη δική του διαχείριση κινδύνου δεδομένων και να επιλέξει τον σωστό πάροχο νέφους, πληρώνοντας παράλληλα τις αρχές της διαφάνειας και της λογοδοσίας.

190 Ο ENISA προσφέρει πληροφορίες ή και μηχανισμούς σχετικούς με τη διαχείριση της ασφάλειας μέσω των SLAs, τα κριτήρια με βάση τα οποία μπορεί ένας πελάτης να επιλέξει έναν πάροχο υπηρεσιών νέφους με αποτελεσματικούς πόρους και υπηρεσίες υψηλής ποιότητας σε συμφέρουσα τιμή, τους κινδύνους και τον αντίκτυπο μιας ενδεχόμενης αποτυχημένης παροχής υπηρεσιών από τον πάροχο, λίστα με αναφορά περιστατικών παραβίασης, λίστα εθελοντικής πιστοποίησης παρόχων υπηρεσιών που πληρούν τα κριτήρια που απαιτούνται για την ασφάλεια στο cloud , λίστα εμπειρογνωμόνων που μπορεί να επικοινωνήσει κάποιος μαζί τους , έναν κατάλογο διαφόρων σχημάτων πιστοποίησης – Cloud Certification Schemes List (CCSL) που μπορεί να ενδιαφέρουν τον οποιοδήποτε πελάτη κ.ά. βλ. ηλ δ/νση https://www.enisa.europa.eu/media/enisa-in-greek/ και https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

191 βλ. Περισσότερα *CNIL*, Recommendations for companies planning to use Cloud computing services, διαθέσιμο στην στην ηλ δ/νση : https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf

αξιολογήσει κατά πόσον οι προβλεπόμενες υπηρεσίες του παρόχου ανταποκρίνονται στα ως άνω. Έπειτα, θα πρέπει να διενεργήσει μία ανάλυση κινδύνων[192] για να αναγνωρίσει τα κατάλληλα μέτρα ασφαλείας που πρέπει να ζητηθούν από τον πάροχο ή/και να εγκαταστήσει εντός της επιχείρησής του ο πελάτης. Μετά, αφού επιλέξει τη σωστή υπηρεσία νέφους (SaaS, IaaS, PaaS), θα πρέπει να καταλήξει στην επιλογή ενός CSP, ο οποίος παρέχει επαρκείς εγγυήσεις (μέτρα ασφαλείας και εμπιστευτικότητας, διαφάνεια σχετικά με τις διαδικασίες και τα μέσα που χρησιμοποιεί (π.χ μεταφορά δεδομένων στο εξωτερικό, συνεργασία με υπεργολάβους) για την προστασία των δεδομένων. Ο πελάτης πρέπει να αξιολογήσει τα νομικά προσόντα του παρόχου και το επίπεδο προστασίας που παρέχει για τα δεδομένα. Τέλος τονίζει την ανάγκη συνεχούς επανεξέτασης της εσωτερικής πολιτικής ασφαλείας, καθώς η χρήση του cloud συνεπάγεται νέους κινδύνους και της συστηματικής παρακολούθησης των διαδικασιών του παρόχου.

3.10.3 Πιστοποιήσεις ISO

Οι πάροχοι υπηρεσιών νέφους, που επιθυμούν να συμμορφωθούν με το Νέο Κανονισμό και να παρέχουν αξιόπιστες υπηρεσίες, δύνανται να “πιστοποιηθούν”, από διάφορα παγκοσμίως αναγνωρισμένα πρότυπα, που διασφαλίζουν την ποιότητα των παρεχόμενων υπηρεσιών, τη λειτουργική ορθότητα της τεχνικής υποδομής τους κ.ά., αυξάνοντας την αξιοπιστία και αποτελεσματικότητα των υπηρεσιών τους.

Ένας τέτοιος οργανισμός που δημιουργεί και εκδίδει διεθνή βιομηχανικά πρότυπα, δηλαδή έγγραφες τεκμηριωμένες συμφωνίες που περιέχουν τεχνικές π.χ προδιαγραφές ή άλλα κριτήρια και χρησιμοποιούνται σαν κανόνες από τις επιχειρήσεις είναι ο Διεθνής Οργανισμός Τυποποίησης (ISO – International Organization for Standardization).

Τα πρότυπα ISO, αποδεικνύουν ότι οι προσφερόμενες από τον πάροχο υπηρεσίες είναι αποδοτικές, σύμφωνες με την κείμενη νομοθεσία και τουλάχιστον συμμορφούμενες με μία συγκεκριμένη δομή διαδικασιών διαχείρισης της ασφάλειας

192 Οι πιο σημαντικοί κίνδυνοι που σχετίζονται με το νέφος, όπως προεκτέθηκε, είναι οι εξής : η έλλειψη διαχείρισης της επεξεργασίας, η τεχνολογική εξάρτηση από τον πάροχο cloud, ελαττώματα στην απομόνωση των δεδομένων, έκθεση των δεδομένων σε δικαστικά αιτήματα αλλοδαπών αρχών, ελαττώματα στις σχέσεις υπεργολαβίας, μη ασφαλής ή αναποτελεσματική καταστροφή των δεδομένων, προβλήματα διαχείρισης και ενίσχυσης των δικαιωμάτων των υποκειμένων, μη διαθεσιμότητα της υπηρεσίας , προβλήματα δικτύου, μη συμμόρφωση με κανονισμούς σχετικούς με τη διαβίβαση των δεδομένων.

των δεδομένων[193]. Έτσι, επιδεικνύουν την ασφάλεια που αναζητά ο πελάτης και την αξιοπιστία των παρεχόμενων υπηρεσιών.

Στο χώρο του cloud computing, το πρότυπο ISO/IEC 27018/2014[194], το οποίο, εν όψει του Κανονισμού 2016/679 (ΕΕ), θα αντικατασταθεί προσεχώς από το ISO/IEC FDIS 27018 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public cloud acting as PII processors, αποτελεί ένα πρότυπο που για τη δημιουργία του λήφθηκε υπόψιν και η Γνώμη 05/2012 για τη νεφοϋπολογιστική της Επιτροπής του άρθρο 29. Καθώς δε η πιστοποίηση που παρέχει, αφορά σε παγκόσμιο επίπεδο, δηλαδή, μπορεί να πιστοποιηθεί και ένας πάροχος που εδρεύει στην Αμερική, διασφαλίζεται η προσπάθεια συμμόρφωσης με το Νέο Κανονισμό και η ενίσχυση της ιδιωτικότητας από όλους.

Το εν λόγω πρότυπο, δημιουργεί ένα κοινό σύνολο κανόνων ασφαλείας και ελέγχων , που μπορεί να εφαρμόσει οποιασδήποτε πάροχος υπολογιστικού νέφους, ως εκτελών την επεξεργασία σε προσωπικά δεδομένα, σύμφωνα με τις αρχές προστασίας αυτών. Σκοπός του είναι η συμμόρφωση του παρόχου με όλες τις υποχρεώσεις που του αναλογούν και η ενίσχυση της διαφάνειας των διαδικασιών του με αποτέλεσμα τη σύναψη της συμφωνίας παροχής υπηρεσιών μεταξύ του παρόχου και του πελάτη.

Βέβαια, η εφαρμογή του προϋποθέτει συνάμα τη χρήση των εξής προτύπων:

- του ISO/IEC 17788/Rec.ITU-TY.3500,Information technology— Cloud computing, Overview and vocabulary, το οποίο παρέχει μία επισκόπηση του cloud computin με ένα σύνολο όρων και ορισμών (αναμένεται επανέκδοσή του),
- του ISO/IEC 27000:2014,Information technology— Security techniques — Information security management systems— Overview and vocabulary, το οποίο θέτει κανόνες και αναλύει τα συστήματα διαχείρισης της ασφάλειας των πληροφοριών στο νέφος,
- του ISO/IEC 27001:2013, Information technology— Security techniques— Information security management systems— Requirements, που καθορίζει τις απαιτήσεις για την αξιολόγηση των κινδύνων και κατ' επέκταση και τη δημιουργία, εφαρμογή, διατήρηση και συνεχή βελτίωση ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών,

193 Η πιστοποίηση με ένα πρότυπο δεν διασφαλίζει την ασφάλεια ούτε εξασφαλίζει την εμπιστοσύνη με τον πελάτη π.χ δεν καλύπτουν θέματα δικαιοδοσίας, υπάρχει ανησυχία ως προς την ικανότητα λογοδοσίας και την ευθύνη των παρόχων σε περιπτώσεις παραβίασης των δεδομένων . Αυτό επιτάσσει την επέκταση των προτύπων. / βλ. περισσότερα, *ENISA* , Certification in the EU Cloud Strategy , σελ 8, διαθέσιμο στην ηλ δ/νση : https://resilience.enisa.europa.eu/cloud-computing-certification/certification-in-the-eu-cloud-strategy

194 βλ. περισσότερα στην ηλ δ/νση : https://www.iso.org/obp/ui/#iso:std:iso-iec:27018:ed-1:v1:en

- του ISO/IEC 27002:2013, Information technology— Security techniques— Code of practice for information security controls, που παρέχει κατευθυντήριες γραμμές στο πλαίσιο εφαρμογής ενός συστήματος διαχείρισης της ασφάλειας των πληροφοριών, και
- του ISO/IEC 29100:2011, Information technology— Security techniques— Privacy framework, το οποίο παρέχει ένα πλαίσιο προστασίας της ιδιωτικότητας, καθορίζοντας μία κοινή ορολογία της έννοιας του "απορρήτου", την ιδιότητα κάθε εμπλεκόμενου φορέα στην επεξεργασία προσωπικών δεδομένων και αναφορές σε γνωστές αρχές προστασίας της ιδιωτικής ζωής στις ΤΠ.

Επομένως, καθώς η εφαρμογή ενός προτύπου ISO προϋποθέτει και την εφαρμογή κάποιου άλλου – συμπληρωματικού, καλύπτονται διάφοροι τομείς που δημιουργούν προβληματισμό στο χώρο του cloud computing σε έναν πελάτη του και ενισχύεται η αξιοπιστία ενός παρόχου[195].

Επίσης, η Ομάδα του άρθρου 29, έχει εκδώσει γνώμη που αφορά στη δημιουργία ενός κώδικα δεοντολογίας, τρία χρόνια πριν την εφαρμογή του Κανονισμού, τονίζοντας μάλιστα και τα "τρωτά" του σημεία αναφορικά με το περιβάλλον του νέφους[196].

3.10.4 Συμβατικές εγγυήσεις στη σχέση μεταξύ παρόχου και πελάτη[197].

Μετά την επιλογή του σωστού παρόχου, ο πελάτης, έχοντας ως γνώμονα την την προστασία των δεδομένων και των δικαιωμάτων των υποκειμένων, πρέπει να διασφαλίσει ένα ελάχιστο περιεχόμενο στη σύμβαση μεταξύ αυτού και του παρόχου, σύμφωνα και με το άρθρο 28 του Κανονισμού 2016/679 (ΕΕ).

Συγκεκριμένα, πρέπει στη σύμβαση αυτή να περιέχονται τουλάχιστον:

1) αναλυτικές και συγκεκριμένες εντολές που δίνει ο πελάτης στον πάροχο, με έμφαση στις SLAs, και τις συναφείς κυρώσεις (αποζημίωση, προσφυγή κλπ) σε περίπτωση παραβίασης αυτής,

2) ακριβή προσδιορισμό των μέτρων ασφαλείας ανάλογα με τους κινδύνους της επεξεργασίας και τη φύση των δεδομένων, ώστε να διασφαλίζεται η ακεραιότητα και διαθεσιμότητα των δεδομένων (π.χ. εφεδρικούς διαδικτυακούς

195 Φυσικά υπάρχουν και άλλα πρότυπα ακόμη και πιο τεχνικά που αφορούν στη δομή και λειτουργία ενός συγκεκριμένου περιβάλλοντος νέφους καθώς και στη διασαφήνιση των ρόλων των εμπλεκόμενων μερών κ.ά / περισσότερα βλ. στην ηλ δ/νση : https://www.iso.org/ics/35.210/x/

196 Διαθέσιμη στην ηλ δ/νση : http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

197 βλ. Αναλυτικά Ομάδα του άρθρου 29 για την προστασία των δεδομένων , Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική , της 1ης Ιουλίου 2012, διαθέσιμη στην ηλεκτρονική δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_el.pdf

συνδέσμους δικτύου, μηχανισμούς πολλαπλής αποθήκευσης και αποτελεσματικής πολλαπλής αποθήκευσης των δεδομένων κ.ά)

3) το κύριο αντικείμενο και η χρονική διάρκεια της σύμβασης παροχής υπηρεσίας, η έκταση, ο τρόπος, ο σκοπός της επεξεργασίας και οι κατηγορίες προσωπικών δεδομένων που υφίστανται την επεξεργασία[198]. Πάλι με αυτόν τον όρο κατανέμονται οι ευθύνες και εξασφαλίζεται ότι τα δεδομένα προσωπικού χαρακτήρα δεν υφίστανται επιπλέον (παράνομη) επεξεργασία για περαιτέρω σκοπούς από αυτούς που έχει ορίσει ο πελάτης.

4) οι ακριβείς προϋποθέσεις επιστροφής των δεδομένων (προσωπικού χαρακτήρα) ή καταστροφής τους μόλις ολοκληρωθεί η παροχή της υπηρεσίας και διαγραφής τους

5) ρήτρες εμπιστευτικότητας, δεσμευτικές, για τον πάροχο, τους υπαλλήλους του και τυχών υπεργολάβους – υποεκτελούντες την επεξεργασία (η πρόσβαση στα δεδομένα επιτρέπεται μόνο σε όσους έχουν σχετική άδεια),

6) ευθεία υποχρέωση του παρόχου στην αρωγή των υποκειμένων, σε οποιαδήποτε επίπεδο τεχνικό και οργανωτικό, άσκησης των δικαιωμάτων τους και διασφάλιση ότι το ίδιο ισχύει και για τη σχέση παρόχου με τον όποιον υπεργολάβο του (δυνατότητα παρέμβασης).

7) ρητοί όροι, δεσμευτικοί για τον πάροχο, που να απαγορεύουν την κοινοποίηση των δεδομένων σε τρίτους εκτός από τους συγκεκριμένους υπεργολάβους του (λήψη γενικής άδειας πρόσληψης ή συνεργασίας με υποεκτελούντα την επεξεργασία και ρητή συναίνεση - συγκατάθεση για όσους ήδη υπάρχουν) και συνάμα υποχρέωση ενημέρωσης του πελάτη για τυχόν αλλαγές ως προς τα πρόσωπα των υπεργολάβων, ώστε να μπορεί αυτός να αντιταχθεί. Επίσης, θα πρέπει να υπάρχει ρητή υποχρέωση του παρόχου, ότι οι συμβάσεις μεταξύ του αυτού και τυχόν υπεργολάβου του (δηλαδή οι υπό-εκτελούντες την επεξεργασία) θα διαλαμβάνουν τις ίδιες ακριβώς συμβατικές ρήτρες– υποχρεώσεις που βαρύνουν και τον ίδιο, ώστε να καθορίζονται με σαφήνεια οι αλυσιδωτές ευθύνες.

Έτσι διασφαλίζεται η διαφάνεια των διαδικασιών και σχέσεων των εμπλεκόμενων φορέων. Ο πελάτης υπηρεσιών νεφοϋπολογιστικής είναι σε θέση να αξιολογεί τη νομιμότητα της επεξεργασίας δεδομένων προσωπικού

198 Όταν ο πάροχος – έχει το ρόλο του εκτελούντος την επεξεργασία ή ο πελάτης έχει αναπτύξει τα δικά του εργαλεία ασφαλείας (σε περιβάλλοντα ιδίως PaaS και IaaS) π.χ κρυπτογράφηση, τυπικά, αγνοεί τα δεδομένα που υπάρχουν στις υπηρεσίες του. Αυτό έχει σαν αποτέλεσμα να μην είναι σε θέση να λάβει τα κατάλληλα υπό συνθήκες (λ.χ αυξημένα μέτρα προστασίας για τα ευαίσθητα δεδομένα) τεχνικά μέτρα ασφαλείας, όπως ψευδωνυμοποίηση , κρυπτογράφηση κ.λ.π./ βλ *ARTICLE 29 DATA PROTECTION WORKING PARTY*, Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, Adopted on 22 September 2015, διαθέσιμη στην ηλεκτρονική δ/νση : https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf

χαρακτήρα εντός του υπολογιστικού νέφους μόνο εάν ο πάροχος τον ενημερώνει για όλα τα συναφή ζητήματα, για όλους τους υπεργολάβους που συμβάλλουν στην παροχή της εκάστοτε υπηρεσίας νεφοϋπολογιστικής, καθώς και για όλες τις τοποθεσίες όπου βρίσκονται κέντρα δεδομένων στα οποία δύναται να γίνεται επεξεργασία δεδομένων προσωπικού χαρακτήρα

8) σαφής καθορισμός των ευθυνών του παρόχου αναφορικά με την ενημέρωση του πελάτη σε περίπτωση παραβίασης δεδομένων του τελευταίου,

9) αναλυτική και ρητή αναφορά εκ μέρους του παρόχου των τοποθεσιών που λαμβάνει χώρα η επεξεργασία των δεδομένων,

10) ειδικός όρος σχετικός με το δικαίωμα του πελάτη να παρακολουθεί τις διαδικασίες επεξεργασίας του παρόχου και την αντίστοιχη υποχρέωση του τελευταίου να συνεργάζεται,

11) υποχρέωση ενημέρωσης του πελάτη από τον πάροχο, σε περίπτωση που ο τελευταίος, προβεί σε αλλαγές σχετικές με την εκάστοτε παρεχόμενη υπηρεσία νέφους π.χ. εκτέλεση πρόσθετων λειτουργιών.

12) καταγραφή και έλεγχος των συναφών διαδικασιών επεξεργασίας δεδομένων προσωπικού χαρακτήρα που επιτελούνται από τον πάροχο υπηρεσιών νεφοϋπολογιστικής ή τους υπεργολάβους.

13) ενημέρωση του πελάτη, 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) υποχρέωση του παρόχου να παρέχει διαβεβαιώσεις ότι οι ρυθμίσεις οργάνωσης και επεξεργασίας δεδομένων που εφαρμόζει ο ίδιος (και οι αντίστοιχες 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[199].

4 Ασφάλεια επεξεργασίας και Εκτίμηση αντίκτυπου (Data Protection Impact Assessment- DPIA)

199βλ. επίσης *CNIL*, Recommendations for companies planning to use Cloud computing services, διαθέσιμο στην στην ηλ δ/νση : https://www.cnil.fr/sites/default/files/typo/document/Recommendations_for_companies_planning_to_use_Cloud_computing_services.pdf , σελ, 8, όπου η γαλλική αρχή παραθέτει λίστα με τους απαραίτητους όρους που πρέπει να διαλαμβάνει ένα συμβόλαιο παροχής υπηρεσιών cloud και “πρότυπα” των εν λόγω συμβατικών ρητρών.

Καταρχάς, προϋπόθεση για την ασφάλεια της επεξεργασίας (άρθρο 32) και τη διενέργεια της εκτίμησης αντικτύπου (άρθρο 35) αποτελεί η τήρηση αρχείου δραστηριοτήτων από τον υπεύθυνο επεξεργασίας, παρόλο που σύμφωνα με τον Κανονισμό, αυτός υποχρεούται στην τήρησή του μόνο αν η επιχείριση ή ο οργανισμός απασχολεί τουλάχιστον 250 εργαζόμενους (άρθρο 30 παρ. 5 Κανονισμού 2016/679/ΕΕ).

Το αρχείο πρέπει να περιλαμβάνει τα ακόλουθα:

- το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας και, κατά περίπτωση, του από κοινού υπεύθυνου επεξεργασίας, του εκπροσώπου του υπεύθυνου επεξεργασίας και του υπεύθυνου προστασίας δεδομένων,
- τους σκοπούς της επεξεργασίας,
- περιγραφή των κατηγοριών υποκειμένων των δεδομένων και των κατηγοριών δεδομένων προσωπικού χαρακτήρα,
- τις κατηγορίες αποδεκτών στους οποίους πρόκειται να γνωστοποιηθούν ή γνωστοποιήθηκαν τα προσωπικά δεδομένα, περιλαμβανομένων των αποδεκτών σε τρίτες χώρες ή διεθνείς οργανισμούς,
- όπου συντρέχει περίπτωση, τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό, συμπεριλαμβανομένων του προσδιορισμού της εν λόγω τρίτης χώρας ή του διεθνούς οργανισμού και, σε περίπτωση διαβιβάσεων απαραίτητων για την εκτέλεση σύμβασης μεταξύ του υποκειμένου των δεδομένων και του υπεύθυνου επεξεργασίας ή για την εφαρμογή προσυμβατικών μέτρων τα οποία λαμβάνονται κατόπιν αιτήματος του υποκειμένου των δεδομένων (άρθρο 49 παρ. 1 εδ. β' Κανονισμού), της τεκμηρίωσης των κατάλληλων εγγυήσεων,
- όπου είναι δυνατό, γενική περιγραφή των τεχνικών και οργανωτικών μέτρων ασφάλειας που αναφέρονται στο άρθρο 32 παρ. 1 του Κανονισμού (βλ. άρθρο 30 παρ. 2 Κανονισμού 2016/679/ΕΕ).

4.1 Ασφάλεια επεξεργασίας

Μία από τις βασικότερες υποχρεώσεις του υπεύθυνου επεξεργασίας και του εκτελούντος αυτή, σύμφωνα με τον Κανονισμό ασφά2016/679 (ΕΕ), είναι η ασφάλεια των προσωπικών δεδομένων και η ενίσχυση των δικαιωμάτων των υποκειμένων. Η ασφάλεια αυτή, αφορά εξίσου στην εμπιστευτικότητα, την ακεραιότητα και τη

διαθεσιμότητα των δεδομένων. Επομένως , είναι δυνατόν να επιτευχθεί, μόνο μέσα από μία εκτίμηση του κινδύνου .

Λαμβάνοντας δε υπόψη, την αυξανόμενη χρήση ψηφιακών ή/και ηλεκτρονικών συστημάτων επεξεργασίας δεδομένων, που συχνά βασίζονται σε υπηρεσίες cloud, οι κίνδυνοι ασφαλείας για προσωπικά δεδομένα συνδέονται σήμερα σε μεγάλο βαθμό με τους κινδύνους ασφάλειας των υποκείμενων δικτύων πληροφορικής και των στοιχείων του συστήματος[200]

Η ασφάλεια των πληροφοριών περιλαμβάνει όλα τα μέτρα που λαμβάνονται για την προστασία τους, όταν υφίστανται επεξεργασία από ένα σύστημα (ηλεκτρονικό ή φυσικό) όπως η μη εξουσιοδοτημένη πρόσβαση, χρήση, διακοπή, τροποποίηση, καταγραφή ή καταστροφή, προκειμένου να διατηρηθεί η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών και όπως αναφέρθηκε ανωτέρω μπορεί να πιστοποιηθεί με τη χρήση διεθνών προτύπων (ISO).

Ωστόσο, η εκτίμηση του κινδύνου[201] που αφορά στην προστασία των δεδομένων, παρόλο που στηρίζεται στην ίδια βάση με αυτή της ασφάλειας των πληροφοριών πρέπει να αξιολογείται διαφορετικά, καθώς δεν διασφαλίζονται αυτόματα και οι κίνδυνοι που μπορεί να προκύψουν για τις ελευθερίες και τα δικαιώματα των υποκειμένων. Η προστασία των προσωπικών δεδομένων ουσιαστικά είναι προστασία των θεμελιωδών δικαιωμάτων των υποκειμένων.[202]

Το άρθρο 32 του Κανονισμού 2016/679 (ΕΕ), αναφέρεται στην ασφάλεια της επεξεργασίας, και ορίζει ότι ο υπεύθυνος και ο εκτελών την επεξεργασία

200 βλ. αναλυτικά ENISA, Guidelines for SMEs on ths security of personal data processing, σελ 8, διαθέσιμη στην ηλ δ/νση : https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

201 Ως “κίνδυνος” νοείται ένα υποθετικό σενάριο που περιγράφει ένα συμβάν και όλες τις απειλές που θα επέτρεπαν να συμβεί . Συμπεριλαμβάνει την πηγή του κινδύνου, τον τρόπο εκμετάλλευσης των ευπαθειών των υποστηρικτικών στοιχείων και το πλαίσιο απειλών σχετικά με τα προσωπικά δεδομένα, καταλήγοντας στις επιπτώσεις στην ιδιωτικότητα των υποκειμένων. / βλ. Αναλυτικά CNIL, Privacy Impact Assessment (PIA) METHODOLOGY, Feb 2018 edition, σελ 8, διαθέσιμη στην ηλεκτρονική δ/νση : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

202 βλ. Αιτιολογική σκέψη 75, όπου ορίζεται ότι οι κίνδυνοι για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, ποικίλης πιθανότητας και σοβαρότητας, είναι δυνατόν να προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα η οποία θα μπορούσε να οδηγήσει σε σωματική, υλική ή μη υλική βλάβη, ιδίως όταν η επεξεργασία μπορεί να οδηγήσει σε διακρίσεις, κατάχρηση ή υποκλοπή ταυτότητας, οικονομική απώλεια, βλάβη φήμης, απώλεια της εμπιστευτικότητας των δεδομένων προσωπικού χαρακτήρα που προστατεύονται από επαγγελματικό απόρρητο, παράνομη άρση της ψευδωνυμοποίησης, ή οποιοδήποτε άλλο σημαντικό οικονομικό ή κοινωνικό μειονέκτημα· όταν τα υποκείμενα των δεδομένων θα μπορούσαν να στερηθούν των δικαιωμάτων και ελευθεριών τους ή να εμποδίζονται από την άσκηση ελέγχου επί των δεδομένων τους προσωπικού χαρακτήρα· όταν υπόκεινται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα τα οποία αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, πολιτικά φρονήματα, θρησκεία ή φιλοσοφικές πεποιθήσεις ή συμμετοχή σε συνδικάτα και γίνεται επεξεργασία γενετικών δεδομένων, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή ή ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας· όταν αξιολογούνται προσωπικές πτυχές, ιδίως όταν επιχειρείται ανάλυση ή πρόβλεψη πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή μετακινήσεις, προκειμένου να δημιουργηθούν ή να χρησιμοποιηθούν προσωπικά προφίλ· όταν υποβάλλονται σε επεξεργασία δεδομένα προσωπικού χαρακτήρα ευάλωτων φυσικών προσώπων, ιδίως παιδιών· ή όταν η επεξεργασία περιλαμβάνει μεγάλη ποσότητα δεδομένων προσωπικού χαρακτήρα και επηρεάζει μεγάλο αριθμό υποκειμένων των δεδομένων.

λαμβάνοντας υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής και τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, εφαρμόζουν κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίζεται το κατάλληλο επίπεδο ασφάλειας έναντι των κινδύνων και μάλιστα σε τακτική βάση πρέπει να επαναπροσδιορίζονται και να επαναξιολογούνται.

Επομένως, η εκτίμηση του κινδύνου για την προστασία των δεδομένων, αποτελεί και αυτή μία κυκλική διαδικασία, που πρακτικά μεθοδεύεται από την οριοθέτηση του πλαισίου (σκοπός επεξεργασίας, είδος δεδομένων, εμπλεκόμενα μέρη) και ακολουθούν ο προσδιορισμός, η ανάλυση, η αξιολόγηση, η διαχείριση και η παρακολούθηση των κινδύνων. Το επίπεδο του κινδύνου προκύπτει από τον συνδυασμό της σοβαρότητας και της πιθανότητας. Η σοβαρότητα αντικατοπτρίζει το μέγεθος του κινδύνου, που εξαρτάται από τον επιζήμιο χαρακτήρα των πιθανών επιπτώσεων σε σχέση με την επεξεργασία των δεδομένων. Η πιθανότητα, αναφέρεται στο ενδεχόμενο εμφάνισης του κινδύνου, που εξαρτάται από το επίπεδο των τρωτών σημείων των υποδομών[203]

Η πιθανότητα του κινδύνου στην ασφάλεια των πληροφοριών παρουσιάζεται ως απειλή για το σύστημα των πόρων Τ.Π., την εκμετάλλευση των ευπαθειών και αδυναμιών του. Η ασφάλεια των δεδομένων, συνακόλουθα, σχετίζεται με τα μέτρα ασφαλείας των πληροφοριών που π.χ. αφορούν στο υλικό και λογισμικό, στα κανάλια μετάδοσης του δικτύου των δεδομένων. Ωστόσο, δεν διασφαλίζεται μόνο με τη λήψη τεχνικών μέτρων. Στην εκτίμηση του κινδύνου που ορίζει το άρθρο 32, πρέπει να ληφθούν υπόψιν και άλλα κριτήρια, όπως τα εμπλεκόμενα μέρη και ο ανθρώπινος παράγοντας. Πρέπει να προσδιοριστούν επακριβώς οι κίνδυνοι για την ασφάλεια των δεδομένων που συνδέονται με τη δραστηριότητα της επεξεργασίας και τα εμπλεκόμενα μέρη. Η ασφάλεια λοιπόν, αφορά όχι μόνο σε ασφάλεια της υποδομής ΤΠ (λογισμικό, υλικό δικτύου κ.ά) αλλά και σε ασφάλεια εγκαταστάσεων ενός οργανισμού ή επιχείρησης (λ.χ εξουσιοδοτημένη πρόσβαση σε χώρους όπου φυλάσσεται το αρχείο, οι οποίοι πρέπει να είναι κλειδωμένοι) και σε διαχείριση ανθρώπινων ενεργειών και πόρων (π.χ κίνδυνος μπορεί να προκύψει γιατί ένας μη εξουσιοδοτημένος υπάλληλος εταιρίας αποκτά μη νόμιμη πρόσβαση σε προσωπικά δεδομένα που αυτή επεξεργάζεται[204], οπότε πρέπει να ληφθούν μέτρα αποτροπής μιας τέτοιας ενέργειας) ώστε να διασφαλιστεί το απόρρητο, η ακεραιότητα και η

203 βλ. Αναλυτικά CNIL, Privacy Impact Assessment (PIA) METHODOLOGY, Feb 2018 edition, σελ 8, διαθέσιμη στην ηλεκτρονική δ/νση : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

204 Bitcom, Risk Assessment & Data Protection Impact Assessment , Guide, διαθέσιμο στην ηλ δ/νση : http://www.digitalestadt.org/bitkom/org/noindex/Publikationen/2017/Leitfaden/170919-LF-Risk-Assessment-ENG-online-final.pdf

διαθεσιμότητα.

Προκειμένου να μειωθεί ο κίνδυνος, ο Κανονισμός υποχρεώνει τον υπεύθυνο και εκτελούντα την επεξεργασία (άρθρο 32 παρ. 2) να εφαρμόζουν τεχνικά μέτρα ασφαλείας, τα οποία συμπεριλαμβάνουν τουλάχιστον κατά περίπτωση την ψευδωνυμοποίηση και την κρυπτογράφηση των δεδομένων προσωπικού χαρακτήρα. Συνάμα ορίζει και την εφαρμογή οργανωτικών μέτρων, μεταξύ των οποίων, η δυνατότητα διασφάλισης του απορρήτου, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση, η δυνατότητα αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος και η διαδικασία για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των μέτρων (ποιος έχει πρόσβαση, ποιος πρέπει να γνωρίζει, τι μέτρο έχει ληφθεί, ποιος είναι υπεύθυνος για την εφαρμογή του και πότε αυτή ολοκληρώνεται, ποιος πρέπει να διεξάγει DPIA κ.ά) .

Κλείνοντας, για τη διασφάλιση της ασφάλειας της επεξεργασίας, πρέπει οι υπεύθυνοι επεξεργασίας και οι εκτελούντες αυτή, να υιοθετήσουν μία εναρμονισμένη προσέγγιση της ανάλυσης και υλοποίησης της ασφάλειας, με πρακτικές κοινά αποδεκτές και εφαρμοστέες από όλους, διαδικασίες αξιολόγησης κινδύνου καλά τεκμηριωμένες και λίστες τεχνικών και οργανωτικών μέτρων δοκιμασμένων και αξιόπιστων. Καθώς ωστόσο οι κίνδυνοι για την προστασία των δεδομένων και οι κίνδυνοι για την προστασία και ασφάλεια των ΤΠ είναι δύο διαφορετικές έννοιες, η ασφάλεια της επεξεργασίας δεν επιτυγχάνεται μόνο μέσα από τη χρήση προτύπων όπως το ISO/IEC 27001, που αναλύθηκε στην προηγούμενη ενότητα αλλά απαιτείται ο συνδυασμός του με τη χρήση και άλλων προτύπων, όπως το ISO/IEC FDIS 29151:2016: Κατευθυντήριες γραμμές για την προστασία των προσωπικών δεδομένων και τα DIN ISO/IEC 27001:2015 και DIN ISO/IEC 27002:2016 ως κατευθυντήρια γραμμή για την ερμηνεία μέτρων[205].

4.2 Εκτίμηση Αντικτύπου (Data Protection Impact Assessment- DPIA)

4.2.1 Νομικό πλαίσιο (άρθρα 35, 40, 42, 83 παρ 4α Κανονισμού 2016/679/ΕΕ)

Ωστόσο, ορισμένες φορές, η συμμόρφωση με τον Κανονισμό δεν επιτυγχάνεται μόνο με όσα προεκτέθηκαν. Για πρώτη φορά αυτός, ορίζει ρητά μία έτερη υποχρέωση του υπεύθυνου επεξεργασίας, στο άρθρο 35 που αφορά στη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων.

205 Bitcom, Risk Assessment & Data Protection Impact Assessment, Guide, σελ 34, διαθέσιμο στην ηλ δ/νση: http://www.digitalestadt.org/bitkom/org/noindex/Publikationen/2017/Leitfaden/170919-LF-Risk-Assessment-ENG-online-final.pdf

Συγκεκριμένα, το άρθρο 35 διαλαμβάνει ότι : "*Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών (*όπως το cloud computing) *και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα και ενδεικτικά στις περιπτώσεις: α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, όπως η κατάρτιση προφίλ (π.χ. πληροφορίες σε σχέση με τα μέσα κοινωνικής δικτύωσης), β) επεξεργασίας μεγάλης κλίμακας των δεδομένων των άρθρων 9 και 10 ΓΚΠΔ και γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα*[206]"

Ο Κανονισμός δεν παρέχει επίσημο ορισμό της DPIA, ορίζει όμως το ελάχιστο περιεχόμενό της, το οποίο πρέπει να περιέχει: α) τη συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και τον σκοπό αυτών, καθώς και του εννόμου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας, β) την εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε σχέση με τους σκοπούς τους, γ) την εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, συμπεριλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφαλείας, ώστε να διασφαλίζεται η προστασία των δεδομένων και να αποδεικνύεται η συμμόρφωση προς τον Κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων όσο και άλλων ενδιαφερόμενων προσώπων[207].

Η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας που αναφέρονται στο άρθρο 40 του Κανονισμού από τους σχετικούς υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία λαμβάνεται δεόντως υπόψιν κατά την εκτίμηση του αντικτύπου των πράξεων επεξεργασίας που εκτελούνται από τους εν λόγω υπευθύνους ή εκτελούντες την επεξεργασία, ιδίως για τους σκοπούς της εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων[208]. Θα πρέπει επίσης να λαμβάνονται υπόψη οι πιστοποιήσεις, οι σφραγίδες και τα σήματα προστασίας των δεδομένων για τον σκοπό της απόδειξης της συμμόρφωσης των πράξεων επεξεργασίας των υπεύθυνων επεξεργασίας και των εκτελούντων την επεξεργασία (άρθρο 42) με τον ΓΚΠΔ, καθώς και οι δεσμευτικοί εταιρικοί κανόνες (BCR).

Η παραβίαση της υποχρέωσης διενέργειας εκτίμησης αντικτύπου από

206 Βλ. άρ. 35 παρ. 1 και 3 Κανονισμού.
207 Αρ. 35 παρ. 7 Κανονισμού 2016/679 (ΕΕ).
208 Βλ. άρ. 35 παρ. 8 Κανονισμού 2016/679 (ΕΕ).

τον υπεύθυνο επεξεργασίας επιφέρει διοικητικά πρόστιμα μέχρι 10.000.000 € ή, στην περίπτωση επιχειρήσεων έως 2% του συνολικού παγκόσμιου ετησίου κύκλου εργασιών[209].

4.2.2 Εφαρμογή Νομικού Πλαισίου.

Καταρχάς, η υποχρέωση των υπεύθυνων επεξεργασίας για τη διενέργεια DPIA θα πρέπει να γίνεται αντιληπτή σε σχέση με τη γενική τους υποχρέωση να διαχειρίζονται με ενδεδειγμένο τρόπο τους κινδύνους που ενέχει η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, για την προάσπιση των δικαιωμάτων και των ελευθεριών του υποκειμένων[210] και να εκτελείται πριν την επεξεργασία. Οπότε απαιτείται η συστηματική και διαρκής εξακρίβωση, ανάλυση, εκτίμηση, αξιολόγηση, αντιμετώπιση των κινδύνων και η τακτική τους επανεξέταση.

Αυτό σημαίνει ότι σε περίπτωση που αρχικά δεν απαιτείται η διενέργεια DPIA, στην πορεία, μπορεί να αλλάξουν οι συνθήκες και αυτή να καταστεί υποχρεωτική, καθώς οι πράξεις επεξεργασίας, ειδικά με τη χρήση νέων τεχνολογιών εξελίσσονται ταχέως και προκύπτουν τρωτά σημεία. Έτσι εφόσον μεταβληθούν οι κίνδυνοι που συνεπάγονται οι πράξεις επεξεργασίας (το πλαίσιο, τα δεδομένα, οι σκοποί, η λειτουργία, οι αποδέκτες, οι πηγή του κινδύνου, ενδεχόμενοι συνδυασμοί δεδομένων, μέτρα ασφαλείας κ.ά) ή το οργανωτικό και κοινωνικό πλαίσιο αυτής, τότε η DPIA είναι υποχρεωτική.

Η διενέργειά της, δύναται να αφορά μία επιμέρους πράξη επεξεργασίας αλλά συνάμα θα μπορούσε να χρησιμοποιηθεί και για την αξιολόγηση περισσότερων πράξεων με παρεμφερές πεδίο εφαρμογής, φύση, πλαίσιο, σκοπό και κινδύνους[211]. Επίσης, μπορεί να χρησιμεύσει στην εκτίμηση του αντικτύπου ενός τεχνολογικού προϊόντος σχετικά με την προστασία των δεδομένων, π.χ. ενός στοιχείου υλισμικού ή λογισμικού, όταν αυτό ενδέχεται να χρησιμοποιηθεί από διαφορετικούς υπεύθυνους επεξεργασίας. Εννοείται πως ο υπεύθυνος επεξεργασίας που κάνει χρήση του προϊόντος παραμένει υποχρεωμένος να διενεργήσει τη δική του ΕΑΠΔ ως προς τη συγκεκριμένη εφαρμογή, ωστόσο, εάν ενδείκνυται, αυτή μπορεί να τεκμηριωθεί με χρήση της ΕΑΠΔ που έχει καταρτίσει ο πάροχος του προϊόντος[212].

209 Αναλυτ. άρ. 83 παρ. 4, α Κανονισμού.

210 Η αναφορά στα δικαιώματα και τις ελευθερίες συμπεριλαμβάνει και τα δικαιώματα προστασίας των δεδομένων και της ιδιωτικής ζωής. Ωστόσο, δεν εξαιρούνται και άλλα θεμελιώδη δικαιώματα όπως π.χ ελευθερία συνείδησης και θρησκείας, λόγου, σκέψης, κυκλοφορίας, απαγόρευση διακρίσεων κ.ά/ βλ. *Ομάδα Εργασία του άρθρου 29 για την προστασία των δεδομένων, WP 248,* Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679 , που εκδόθηκαν την 04.04.2017, όπως τελικά αναθεωρήθηκαν και εκδόθηκαν την 4 Οκτωβρίου 2017, διαθέσιμη στην ηλεκτρονική δ/νση : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

211 Βλ .άρθρο 35 παρ 1 και αιτιολογική σκέψη 92 Κανονισμού 2016/679 (ΕΕ).

212 βλ. αναλυτικά *Ομάδα Εργασίας του άρθρου 29 για την προστασία των δεδομένων*, WP248 αναθ 01,

Ωστόσο, η διενέργεια σε κάθε περίπτωση (είτε απαιτείται υποχρεωτικά είτε όχι) DPIA , είναι πάντα χρήσιμη για τον υπεύθυνο επεξεργασίας και επιδεικνύει την προσπάθεια και θέλησή του για συμμόρφωση με τον Κανονισμό.

4.2.2.1 Πότε μία πράξη επεξεργασίας "ενδέχεται να επιφέρει υψηλό κίνδυνο"

Ο Κανονισμός δεν απαιτεί τη διενέργεια DPIA για κάθε πράξη επεξεργασίας. Επομένως, αυτή δεν είναι αναγκαία όταν η επεξεργασία ΔΕΝ "ενδέχεται να επιφέρει υψηλό κίνδυνο "ή διατίθεται παρόμοια DPIA ή έχει εγκριθεί πριν την έναρξη ισχύος του Κανονισμού ή διαθέτει νομική βάση ή περιλαμβάνεται στον κατάλογο πράξεων επεξεργασίας που εκδίδει η ΑΠΔΠΧ,για τις οποίες δεν απαιτείται DPIA (βλ. άρ. 35 παρ. 5 Κανονισμού 2016/679 (ΕΕ). Ωστόσο στις εν λόγω περιπτώσεις, ο υπεύθυνος επεξεργασίας θα πρέπει να δικαιολογεί και να τεκμηριώνει τους λόγους μη διενέργειας και να καταγράφει και τις απόψεις του υπεύθυνου προστασίας.

Στο άρθρο 35, αναφέρονται ενδεικτικά πράξεις που δύνανται να επιφέρουν υψηλό κίνδυνο, ιδίως στην περίπτωση που εισάγεται μία νέα τεχνολογία επεξεργασίας δεδομένων[213].

Η Ομάδα Εργασίας του άρθρου 29, για να βοηθήσει τον υπεύθυνο επεξεργασίας, έχει εκδώσει λίστα κριτηρίων, που πρέπει να λαμβάνονται υπόψιν κατά τον προσδιορισμό του "υψηλού κινδύνου". Όσο περισσότερα από αυτά πληρούνται τόσο πιθανότερη η ύπαρξη υψηλού κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Πιο συγκεκριμένα :

1) αξιολόγηση ή βαθμολόγηση, περιλαμβανομένης της κατάρτισης προφίλ και προβλέψεων, ιδίως *«πτυχών που αφορούν τις επιδόσεις στην εργασία, την οικονομική κατάσταση, την υγεία, τις προσωπικές προτιμήσεις ή συμφέροντα, την αξιοπιστία ή τη συμπεριφορά, τη θέση ή κινήσεις του υποκειμένου των δεδομένων»* (αιτιολογικές σκέψεις 71 και 91),
2) λήψη αυτοματοποιημένων αποφάσεων που παράγουν έννομα αποτελέσματα ή σημαντικά αποτελέσματα κατά ανάλογο τρόπο (άρθρο 35 παρ 3 στοιχ α΄),
3) συστηματική[214] παρακολούθηση, παρατήρηση ή έλεγχος των υποκειμένων, περιλαμβανομένων των δεδομένων που συλλέγονται μέσω δικτύων (άρθρο 35 παρ. 3 στοιχ γ΄), ιδίως σε δημόσια προσβάσιμο χώρο, που σημαίνει ότι τα υποκείμενα ενδέχεται να αγνοούν τη συλλογή των δεδομένων τους,

---

Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679., όπως εκδόθηκαν στις 4 Απριλίου 2017 και όπως τελικά αναθεωρήθηκαν και εκδόθηκαν στις 4 Οκτωβρίου 2017, διαθέσιμη στην ηλεκτρονική δ/νδη : http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

213 βλ. Αιτιολογικές σκέψεις 89, 91 Κανονισμού 2016/679 (ΕΕ).

214Με τον όρο συστηματική χαρακτηρίζεται η παρακολούθηση η οποία λαμβάνει χώρα σύμφωνα με ένα σύστημα ή είναι προκαθορισμένη, οργανωμένη ή μεθοδική, ή υλοποιείται στο πλαίσιο γενικού σχεδίου συλλογής δεδομένων ή διενεργείται στο πλαίσιο στρατηγικής ή και όλα τα παραπάνω.

4) ευαίσθητα δεδομένα ή δεδομένα εξαιρετικά προσωπικού χαρακτήρα (άρθρα 9 και 10)[215],
5) δεδομένα μεγάλης κλίμακας επεξεργασίας[216],
6) δεδομένα που αφορούν σε ευάλωτα υποκείμενα δεδομένων, εξαιτίας της άνισης σχέσης ισχύος μεταξύ των υποκειμένων και του υπεύθυνου επεξεργασίας[217], που μπορεί να συνεπάγεται την αδυναμία των υποκειμένων να αρνηθούν στην επεξεργασία,
7) η αντιστοίχιση ή ο συνδυασμός δεδομένων που απορρέουν από περισσότερες πράξεις επεξεργασίας που υλοποιούνται για διαφορετικούς σκοπούς και/ή από διαφορετικούς υπεύθυνους επεξεργασίας , με τρόπο που αγνοεί το υποκείμενο των δεδομένων ,
8) η καινοτόμος χρήση ή εφαρμογή νέων τεχνολογικών ή οργανωτικών λύσεων π.χ η συνδυασμένη χρήση των δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου για βελτιωμένο φυσικό έλεγχο πρόσβασης[218] και
9) όταν η επεξεργασία εμποδίζει τα υποκείμενα των δεδομένων να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μία υπηρεσία ή σύμβαση[219].

4.2.2.2 Πότε και από ποιον διενεργείται η DPIA

Η DPIA πρέπει να διενεργείται πάντα πριν ξεκινήσει η επεξεργασία δεδομένων, ακόμη και αν κάποια πράξη της στο αρχικό αυτό στάδιο είναι άγνωστη, αφού αποτελεί βάση για τη λήψη αποφάσεων σχετικά με την επεξεργασία.

Είναι δε, μία διαρκής διαδικασία που επικαιροποιείται και επανεξετάζεται σε περίπτωση μεταβολής κίνδυνου ή εάν επέλθει κάποια σημαντική αλλαγή κατά τη διάρκεια και στη διαδικασία της επεξεργασίας.

Την ευθύνη – απόφαση διενέργειας , έχει/λαμβάνει ο υπεύθυνος επεξεργασίας[220]. Ωστόσο, στην υλοποίησή της δύναται να συνδράμει και ο εκτελών

215 Σε αυτή την κατηγορία ενδέχεται να υπαχθούν και δεδομένα τα οποία χαρακτηρίζονται ως ευαίσθητα διότι συνδέονται με τις δραστηριότητες του ιδιωτικού βίου (π.χ οι ηλεκτρονικές επικοινωνίες η εμπιστευτικότητα των οποίων πρέπει να διαφυλάσσεται) ή επηρεάζουν την άσκηση ενός θεμελιώδους δικαιώματος (π.χ δεδομένα τοποθεσίας, τα οποία περιορίζουν την ελευθερία της κυκλοφορίας) ή η παραβίασή τους σαφώς επηρεάζει σημαντικά την καθημερινή ζωή του υποκειμένου (οικονομικά δεδομένα, που μπορεί να εκμεταλλευτεί κάποιος για την τέλεση απάτης πληρωμών), ή προσωπικά έγγραφα, μηνύματα ηλεκτρονικού ταχυδρομείου, ημερολόγια, σημειώσεις από ηλεκτρονικό αναγνώστη (e-reader) που προσφέρει δυνατότητες τήρησης σημειώσεων, και πολύ προσωπικές πληροφορίες που περιλαμβάνονται σε εφαρμογές καταγραφής βίου («life-logging»).

216 βλ. αιτιολογική σκέψη 91, η οποία χαρακτηρίζει μία επεξεργασία “μεγάλης κλίμακας” ,με βάση τον αριθμό των εμπλεκόμενων υποκειμένων των δεδομένων (ως αριθμό ή ως ποσοστό επί του συναφούς πληθυσμού), τον όγκο των δεδομένων, τη διάρκεια ή το μόνιμο χαρακτήρα της δραστηριότητας επεξεργασίας και το γεωγραφικό εύρος αυτής.

217 βλ. αιτιολογική σκέψη 75,

218 βλ. Άρθρο 35 παρ 1 και αιτιολογικές σκέψεις 89 και 91, όπου γίνεται ρητή μνεία στα υφιστάμενα επίπεδα τεχνολογικής γνώσης και τη χρήση νέων τεχνολογιών.

219 βλ. αιτιολογικές σκέψεις 22 και 91

220 Όταν στην πράξη επεξεργασίας συμπράττουν από κοινού υπεύθυνοι επεξεργασίας, θα πρέπει να

την επεξεργασία αλλά να παράσχει συμβουλές όπου και όταν υπάρχει και ο DP . Επιπρόσθετα, κατά περίπτωση ο υπεύθυνος επεξεργασίας δύναται να ζητήσει και τη γνώμη των υποκειμένων των δεδομένων, με την επιφύλαξη της προστασίας εμπορικών ή δημόσιων συμφερόντων ή της ασφάλειας των πράξεων επεξεργασίας[221.]

Η εθνική Εποπτική Αρχή για να διευκολύνει το έργο των υπευθύνων επεξεργασίας αναφορικά με τη διενέργεια DPIA συντάσσει και δημοσιεύει κατάλογο με τις πράξεις επεξεργασίας που υποχρεωτικά υπόκεινται σε προηγούμενη διενέργεια αντικτύπου αλλά και προαιρετικά αυτών που εξαιρούνται από αυτήν.

Ο υπεύθυνος επεξεργασίας, ζητεί τη γνώμη της εποπτικής αρχής πριν την επεξεργασία, όταν οι κίνδυνοι από την επεξεργασία δεν μπορούν να μετριαστούν και να αντιμετωπιστούν επαρκώς (λ.χ. μη εύρεση επαρκών μέτρων αντιμετώπισης των κινδύνων όσον αφορά τις διαθέσιμες τεχνολογίες[222] και το κόστος εφαρμογής, ενδεχόμενο για σημαντικές ή μη αναστρέψιμες συνέπειες για τα φυσικά πρόσωπα) ή όταν το εθνικό δίκαιο επιβάλλει την προηγούμενη διαβούλευση ή/ και τη λήψη προηγούμενης άδειας από την Εποπτική Αρχή. Όταν η Εποπτική Αρχή φρονεί ότι η σχεδιαζόμενη επεξεργασία παραβιάζει τον Κανονισμό, ιδίως αν ο υπεύθυνος επεξεργασίας δεν έχει προσδιορίσει ή μετριάσει επαρκώς τον κίνδυνο, παρέχει σε αυτόν εγγράφως συμβουλές[223].

Τέλος , για τη σωστή και ολοκληρωμένη διενέργειά της, ο υπεύθυνος επεξεργασίας θα μπορούσε να ζητά τη γνώμη και ανεξάρτητων εμπειρογνωμόνων από διάφορα επαγγέλματα (δικηγόρους, IT, επαγγελματίες σε θέματα ασφαλείας ΤΠ, κοινωνιολόγους κ.ά).

4.2.3 Πώς διενεργείται η DPIA

Καταρχάς, η προσέγγιση συμμόρφωσης που εφαρμόζεται με τη διεξαγωγή της DPIA, βασίζεται σε δύο βάσεις: α.- τα θεμελιώδη δικαιώματα και αρχές επεξεργασίας που είναι μη διαπραγματεύσιμα, βασίζονται στο Νόμο και πρέπει να τηρούνται και να διασφαλίζονται ανεξάρτητα από τη φύση, τη σοβαρότητα και πιθανότητα των κινδύνων και β.- τη διαχείριση των κινδύνων για την ιδιωτική ζωή, η

προσδιορίζονται με ακρίβεια οι υποχρεώσεις που αντιστοιχούν στον καθένα και να ορίζεται το μέρος που είναι αρμόδιο για τα διάφορα μέτρα που έχουν σχεδιαστεί για την αντιμετώπιση των κινδύνων και τη διαφύλαξη των δικαιωμάτων και ελευθεριών των υποκειμένων. Ωστόσο, ο καθένας θα πρέπει να διατυπώνει τις ανάγκες του και να ανταλλάσσει χρήσιμες πληροφορίες χωρίς να θέτει σε κίνδυνο τις απόρρητες ή να γνωστοποιεί τρωτά σημεία.

221 Βλ. άρ. 35 παρ. 9 Κανονισμού2016/679 (ΕΕ).

222 Η ψευδωνυμοποίηση και η κρυπτογράφηση στις οποίες ο Κανονισμός αναφέρεται ρητά, δεν αποτελούν οπωσδήποτε τα ενδεδειγμένα μέτρα ασφαλείας, αλλά ένα παράδειγμα αυτών. Τα ενδεδειγμένα μέτρα εξαρτώνται από τη συγκεκριμένη περίπτωση και τους κινδύνους που ελλοχεύουν από κάθε συγκεκριμένη πράξη επεξεργασίας.

223 Βλ. άρθρο 36 Κανονισμού Προηγούμενη διαβούλευση και αναλυτικότερα αιτιολογική σκέψη EU Γενικού Κανονισμού 94, διαθέσιμη στην ηλ. δ/νση https://gdpr-info.eu/recitals/no-94/.

οποία καθορίζει τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την προστασία των δεδομένων[224].

Για να πραγματοποιηθεί μία DPIA είναι απαραίτητο να:

i) καθοριστεί και οριοθετηθεί αναλυτικά το περιεχόμενο - πλαίσιο της επεξεργασίας των προσωπικών δεδομένων,

ii) αναλυθούν οι έλεγχοι, οι οποίοι εγγυώνται τη συμμόρφωση με τις θεμελιώδεις αρχές της αναλογικότητας, της αναγκαιότητας της επεξεργασίας και την προστασία των δικαιωμάτων των υποκειμένων,

iii) αξιολογηθούν οι κίνδυνοι για την ιδιωτική ζωή που συνδέονται με την ασφάλεια των δεδομένων, ώστε να διασφαλιστεί η κατάλληλη αντιμετώπισή τους και

iv) τελικά να τεκμηριωθεί επίσημα σε έγγραφο ή να γίνει επανέλεγχος και αναθεώρηση κάποιων προηγούμενων βημάτων.

Ο Κανονισμός, δεν προσδιορίζει κάποια συγκεκριμένη διαδικασία για τη διενέργειά της, παρά μόνο ορίζει το ελάχιστο περιεχόμενό της στο άρθρο 35 παρ 7.

Στην Ευρώπη και σε διεθνές επίπεδο, οι αρμόδιες αρχές , σε συνεργασία με την ISO, που ασχολούνται και πριν τον Κανονισμό με τη διαχείριση των κινδύνων και την εκτίμηση των επιπτώσεων στην προστασία των δεδομένων, έχουν αναπτύξει και δημοσιεύσει προτάσεις που διευκολύνουν τη διενέργεια της DPIA, με γνώμονα τις κατευθυντήριες γραμμές της Ομάδας του άρθρου 29, όπως:

– FR (Γαλλία): Εκτίμηση Επιπτώσεων στην Ιδιωτικότητα (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015[225]
https://www.cnil.fr/en/privacy-impact-assessment-pia

– HB (Ηνωμένο Βασίλειο): Κώδικας πρακτικής για τη διενέργεια εκτίμησης επιπτώσεων στην ιδιωτικότητα, Γραφείο Επιτρόπου Πληροφοριών (ICO), 2014[226]
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-

224 βλ. αναλυτικά CNIL, Privacy Impact Assessment (PIA) Methodology, Feb. 2018 edition σελ 5, διαθέσιμη στην ηλεκτρονική δ/νση : https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf

225Μάλιστα η CNIL, έχει εκδώσει και ένα λογισμικό ανοιχτού κώδικα, για τη διενέργεια της DPIA, που μπορεί ο οποιοσδήποτε να κατεβάσει στον υπολογιστή του ελεύθερα, διαθέσιμο στην ηλ δ/νση: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment.

226Η ICO έχει εκδώσει και σε μορφή εγγράφου, ένα πρότυπο ως παράδειγμα για την καταγραφή των διαδικασιών και βημάτων της DPIA και το τελικό αποτέλεσμα αυτής, διαθέσιμο στην ηλ δ/ νση : https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

assessments/

– Το ISO/IEC FDIS 29134:2017 – Information technology -- Security techniques- Guidelines for privacy impact assessment[227], (το οποίο συνάδει με τις κατευθυντήριες γραμμές της CNIL) https://www.iso.org/standard/62289.html

Το ως άνω πρότυπο παρέχει οδηγίες για την αξιολόγηση των επιπτώσεων στην ιδιωτική ζωή (που μπορεί να προκύψουν σε συμμόρφωση ή κατά παράβαση των απαιτήσεων για την προστασία της ιδιωτικότητας) μιας διαδικασίας, ενός συστήματος πληροφοριών, ενός προγράμματος, μιας ενότητας λογισμικού, μιας συσκευής ή άλλης πρωτοβουλίας που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, καταδεικνύει τις απαραίτητες ενέργειες για την αντιμετώπιση του κινδύνου, λαμβάνοντας υπόψιν τα εμπλεκόμενα μέρη και παρέχει οδηγίες για τη δομή και το περιεχόμενο μιας έκθεσης DPIA.

Απευθύνεται σε όλους τους τύπους και μεγέθη εταιριών και αφορά τα άτομα που εμπλέκονται στο σχεδιασμό και την υλοποίηση έργων, συμπεριλαμβανομένων εκείνων που χειρίζονται συστήματα ή υπηρεσίες επεξεργασίας δεδομένων προσωπικού χαρακτήρα.

σε συνδυασμό με:

– Το ISO/ IEC 27005:2011 Information Technology – Security techniques – Information Security Risk management , το οποίο προσφέρει μία ολοκληρωμένη προσέγγιση μεταξύ της προστασίας των δεδομένων και της ασφάλειας των πληροφοριών.
https://www.iso.org/standard/56742.html

Μία ολοκληρωμένη και τεκμηριωμένη εκτίμηση αντικτύπου πρέπει να αποτελείται από τα ακόλουθα βήματα[228]:

1) τη γενική μελέτη του πλαισίου της επεξεργασίας και την αιτιολόγηση της ανάγκης διενέργειας DPIA:

α) Αρχικά, πρέπει να καταγράφεται μία γενική μελέτη του πλαισίου της

227Συνδυαστικά με το εν λόγω πρότυπο απαιτούνται και τα: IS Guide73:2009, *Risk management-Vocabulary*, ISO/IEC 27000:2016, *Information technology - Security techniques - Information security management systems - Overview and vocabulary και* ISO/IE 29100:2011, *Information technology - Security techniques -Privacy framework*

228 βλ. Αναλυτικά CNIL, PIA Methodology, Feb 2018 edition, διαθέσιμο στην ηλεκτρονική δ/νση : https://www.cnil.fr/en/privacy-impact-assessment-pia

επεξεργασίας. Δηλαδή, να διενεργείται μία ανάλυση και συστηματική περιγραφή των πράξεων της υπό υλοποίηση επεξεργασίας, λαμβανομένων υπόψιν της φύσης, έκτασης, του πλαισίου[229] και των σκοπών[230] της και να αιτιολογούνται[231].

Δηλαδή θα πρέπει να δοθούν απαντήσεις σε μία σειρά από ερωτήματα όπως: σε τι υποκείμενα θα αφορούν τα προσωπικά δεδομένα; Περιλαμβάνονται και παιδιά ή ευαίσθητες ομάδες; Πόσο έλεγχο θα έχουν επί των δεδομένων; Έχουν εκτιμηθεί προηγουμένως κάποιοι συγκεκριμένοι κίνδυνοι που να αφορούν σε αυτό το είδος της επεξεργασίας; Ποια η τρέχουσα κατάσταση της τεχνολογίας σε αυτό τον τομέα;

Επιπροσθέτως, θα αναλυθούν τα νόμιμα συμφέροντα του υπεύθυνου επεξεργασίας.

Βέβαια, πρέπει να γίνει κατανομή των ρόλων με σαφήνεια και να κατονομάζονται ο/οι υπεύθυνος επεξεργασίας και ο/οι εκτελών/ούντες την επεξεργασία καθώς και αν θα ζητηθεί η παροχή συμβουλών από τον DPO ή κάποιον IT , ήτοι να ορίζεται εν γένει η ομάδα που θα διεξάγει την DPIA.

Τέλος, θα γίνεται ρητή αναφορά σε τυχόν συμμόρφωση με κώδικες δεοντολογίας, πολιτικές ασφαλείας, τομεακά νομικά πρότυπα κ.ά., ώστε να επιδεικνύεται η θέληση και η προσπάθεια για συμμόρφωση με τις θεμελιώδεις αρχές.

β) Ακολουθεί η καταγραφή των προσωπικών δεδομένων, που και πώς θα συλλέγονται για την επεξεργασία, αν θα μοιράζονται ή διαβιβάζονται (τυχόν αποδέκτες) και η διάρκεια αποθήκευσής τους (αιτιολόγηση και περιγραφή μηχανισμών διαγραφής μετά το πέρας αυτής)

Παραδείγματος χάριν θα απαντώνται ερωτήματα όπως τι είδους προσωπικά δεδομένα θα συλλεγούν (απλά, ευαίσθητα, δεδομένα που αντιμετωπίζονται ως ευαίσθητα – βιομετρικά, αριθμός κοινωνικής ασφάλισης, οικονομικά-τεχνικά αρχεία καταγραφής, γεωεντοπισμός κ.ά), πόσο συχνά θα συλλέγονται, πόσο θα διατηρούνται, πόσα άτομα– υποκείμενα αφορούν, τι γεωγραφική περιοχή καλύπτουν, ποιοι οι παραλήπτες; Επιπλέον, θα πρέπει να καταγράφεται μία λειτουργική περιγραφή της πράξης επεξεργασίας και να προσδιορίζονται όλα πληροφοριακά συστήματα και στοιχεία του ενεργητικού στα οποία εναποτίθενται τα δεδομένα (υλισμικό, λογισμικό, δίκτυα, πρόσωπα,

229 περισσότερα βλ αναλυτικά : ICO, Sample DPIA template, διαθέσιμο στην ηλεκτρονική δ/νση : https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

230 Μία αναλυτική καταγραφή των σκοπών της επεξεργασίας περιλαμβάνεται ήδη στο αρχείο δραστηριοτήτων , που τηρεί ο υπεύθυνος επεξεργασίας.

231 Θα πρέπει δηλαδή να εκτιμάται η αναγκαιότητα και η καταλληλότητα της επεξεργασίας σε σχέση με τους σκοπούς της.

έντυπα, δίαυλοι διαβίβασης εντύπων) σε ολόκληρο τον κύκλο ζωής τους (από τη συλλογή μέχρι τη διαγραφή).

2) την τήρηση της νομιμότητας και τη Μελέτη των Θεμελιωδών Αρχών επεξεργασίας , ώστε να διασφαλίζεται η προστασία της ιδιωτικής ζωής[232]

a) Σε πρώτο στάδιο πρέπει να γίνει μία αξιολόγηση των μέτρων που εγγυώνται τη νομιμότητα, την αναλογικότητα και την αναγκαιότητα της επεξεργασίας (άρθρο 35 παρ 7 στοιχ β΄).

Έτσι, θα καταγραφούν και αιτιολογηθούν οι νόμιμες βάσεις της επεξεργασίας, δηλαδή αν το υποκείμενο έχει δώσει τη συγκατάθεσή του για την επεξεργασία των προσωπικών του δεδομένων σε σχέση με τον συγκεκριμένο σκοπό, αν η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης ή για την εκπλήρωση νόμιμης υποχρέωσης του υπεύθυνου επεξεργασίας, ή για την εκτέλεση καθήκοντος προς το δημόσιο συμφέρον ή για άλλους νόμιμους σκοπούς των εννόμων συμφερόντων του υπεύθυνου επεξεργασίας[233].

Έπειτα, θα καταγραφούν και αιτιολογηθούν οι σκοποί της επεξεργασίας, ώστε να συνάδουν με:

- το άρθρο 5 παρ. 1 στοιχ β΄, δηλαδή τον περιορισμό του σκοπού (καθορισμένος, ρητός και νόμιμος),
- το άρθρο 6, δηλαδή την βάση της νομιμότητας της επεξεργασίας και απαγόρευση της κατάχρησης,
- το άρθρο 5 παρ. 1 στοιχ γ΄, δηλαδή την αρχή της ελαχιστοποίησης των δεδομένων (κατάλληλα, συναφή και περιορισμένα στα αναγκαία),
- το άρθρο 5 παρ. 1 στοιχ δ΄, δηλαδή την ποιότητα - ακρίβεια των δεδομένων (επικαιροποίηση) και
- το άρθρο 5 παρ. 1 στοιχ. ε΄, δηλαδή τον περιορισμό της περιόδου αποθήκευσης (διατηρούνται μόνο για το αναγκαίο χρονικό διάστημα που απαιτείται για τους σκοπούς της επεξεργασίας).

b) Έπεται, η αξιολόγηση των μέτρων (που υπάρχουν ή σχεδιάζονται) που συμβάλλουν στην προστασία των δικαιωμάτων των υποκειμένων και δη η καταγραφή και επεξήγηση του τρόπου με τον οποίο αυτά θα εφαρμοστούν[234].

---

232 Στο στάδιο αυτό, πρέπει να απαντηθούν τα εξής ερωτήματα: ποια είναι η νόμιμη βάση της επεξεργασίας; Η επεξεργασία επιτυγχάνει πραγματικά τον σκοπό; Υπάρχει άλλος τρόπος ώστε να επιτευχθεί το ίδιο αποτέλεσμα; Πώς θα εξασφαλιστεί η ποιότητα και η ελαχιστοποίηση των δεδομένων; Ποιες πληροφορίες θα δοθούν στα υποκείμενα; Πώς θα θα βοηθήσουμε στην υποστήριξη των δικαιωμάτων τους; Τι μέτρα λαμβάνονται ώστε να διασφαλιστεί η συμμόρφωση και των εκτελούντων την επεξεργασία;/ βλ περισσότερα *ICO*, Sample DPIA template, διαθέσιμη στην ηλεκτρονική δ/νση : https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

233 βλ αναλυτικά άρθρο 6 Κανονισμού 2016/679 (ΕΕ).

234 Φυσικά θα πρέπει να λαμβάνονται και μέτρα που ορίζουν την εύκολη άσκηση των δικαιωμάτων των

Πιο συγκεκριμένα, ελέγχεται και αξιολογείται αν συμμορφώνονται με:

- την ενημέρωση του υποκειμένου (δίκαιη και διαφανής επεξεργασία, σύμφωνα με τα άρθρα 12, 13 και 14[235]), δηλαδή: παρουσίαση με ευανάγνωστο και κατανοητό τρόπο στο υποκείμενο των όρων χρήσης και εμπιστευτικότητας, της δυνατότητας πρόσβασης σε αυτούς τους όρους, την ύπαρξης συγκεκριμένων ρητρών για τη συσκευή, λεπτομερή παρουσίαση των σκοπών επεξεργασίας και των συλλεγόμενων προσωπικών δεδομένων, παρουσίαση οποιασδήποτε πρόσβασης στα αναγνωριστικά της συσκευής (smartphone/tablet/P.C.) καθορίζοντας συνάμα αν αυτά γνωστοποιούνται ή διαβιβάζονται σε τρίτους και γιατί και ποιοι είναι αυτοί, πληροφορίες σχετικά με τη μέθοδο ασφαλούς αποθήκευσης, ρυθμίσεις επικοινωνίας με την εταιρία/οργανισμός, σχετικά θέματα εμπιστευτικότητας, πληροφορίες σχετικά με τον τρόπο τροποποίησης των προσωπικών δεδομένων
- τη λήψη της συγκατάθεσης του υποκειμένων, η οποία πρέπει να είναι ρητή και να δύναται να ανακληθεί ανά πάσα στιγμή (άρθρα 7 και 8) και αιτιολόγηση των περιπτώσεων στις οποίες αυτή, δεν είναι απαραίτητη. Η συγκατάθεση πρέπει να παρουσιάζεται με απλή και κατανοητή γλώσσα/εικονίδιο, προσαρμοσμένη στον εκάστοτε χρήστη (παιδιά– όπου σε περίπτωση ανηλικότητας αυτή θα πρέπει να δίνεται από τον ασκούντα τη γονική μέριμνα), να δίνεται πριν την επεξεργασία, μετά από ένα μεγάλο χρονικό διάστημα μη χρήσης αυτή να ζητείται εκ νέου, όπου ο χρήστης έχει συναινέσει στην επεξεργασία ειδικών κατηγοριών δεδομένων (π.χ της τοποθεσίας του) θα πρέπει η διεπαφή να δηλώνει ότι διενεργείται η εν λόγω επεξεργασία (με φως ή εικονίδιο), όταν ο χρήστης αλλάζει συσκευή ή διαγράφει τα cookies, θα πρέπει να διατηρούνται οι ρυθμίσεις που σχετίζονται με την τελευταία ενέργειά του– συγκατάθεσή του ,
- την άσκηση του δικαιώματος πρόσβασης (άρθρο 15 που αφορά λ.χ σε δυνατότητα πρόσβασης στο σύνολο των προσωπικών δεδομένων του χρήστη μέσω κοινών διεπαφών, ή λήψης/download αρχείου του συνόλου των προσωπικών του δεδομένων ή πρόσβαση μέσω ελεγχόμενης εισόδου στο ιστορικό του χρήστη και τα ίχνη που έχει αφήσει) και φορητότητας των δεδομένων (άρθρο 20, λ.χ. πρόβλεψη δυνατότητας ανάκτησης, σε μορφή εύκολα επαναχρησιμοποιήσιμης των προσωπικών δεδομένων του χρήστη ώστε να μεταφέρονται σε άλλη υπηρεσία),

υποκειμένων (μέσω τηλεφώνου, έγγραφης φόρμας, μέσω μιας ηλεκτρονικής φόρμας, μέσω e-mail κ.ά)

235βλ αναλυτικά CNIL, Privacy Impact Assessment (PIA) TEMPLATES, Febuary 2018 , διαθέσιμη στην ηλεκτρονική δ/νση : https://www.cnil.fr/en/privacy-impact-assessment-pia

- την άσκηση των δικαιωμάτων διόρθωσης και διαγραφής (άρθρα 16 και 17 αντίστοιχα), δηλαδή καταγραφή των διαδικασιών για τη διόρθωση και τη διαγραφή αυτών, αναγραφή των προσωπικών δεδομένων που θα αποθηκευθούν (τεχνικές προϋποθέσεις, νομικές υποχρεώσεις, μέτρα που πρέπει να λάβει ίσως ο ίδιος ο χρήστης ενέργειες στις οποίες να προβεί με απλά βήματα και καθαρές ενδείξεις κ.ά)
- την άσκηση του δικαιώματος περιορισμού της επεξεργασίας και αντίκρουσης (άρθρα 18 και 21 αντίστοιχα), δηλαδή καταγραφή διαδικασιών που αφορούν στην ύπαρξη πολιτικής ασφαλείας και απορρήτου, ενεργοποιημένες ρυθμίσεις απορρήτου και κατά την εγγραφή και μετά από αυτή, καταγραφή μηχανισμούς ελέγχου της γονικής συναίνεσης για ανηλίκους, συμμόρφωση όσον αφορά στην παρακολούθηση του χρήστη (cookies, διαφήμιση), υιοθέτηση μηχανισμών αποκλεισμού παρακολούθησης παιδιών και κατάρτισης αυτοματοποιημένου προφίλ, μηχανισμός τερματισμού της επεξεργασίας όταν το υποκείμενο ανακαλέσει τη συγκατάθεσή του.
- τη συμμόρφωση με τις υποχρεώσεις που αφορούν στις διαβιβάσεις δεδομένων (άρθρα 44 και 49). Αναλυτική καταγραφή του τόπου αποθήκευσης των δεδομένων (εντός , εκτός Ε.Ε.), σε χώρα που παρέχει επαρκή προστασία και εγγυήσεις, τρίτη χώρα και αιτιολόγηση και εποπτεία (τυποποιημένες συμβατικές ρήτρες, δεσμευτικοί εταιρικοί κανόνες)
- επίσης θα πρέπει να καταγράφεται αν έχει προηγηθεί διαβούλευση (άρθρο 36).

Φυσικά, σε κάθε στάδιο, μετά την καταγραφή των ενεργειών- μέτρων, ακολουθεί έλεγχος συμμόρφωσής του με τον Κανονισμό και ανταπόκρισης στις υποχρεώσεις που αυτός ορίζει. Ανάλογα με το αποτέλεσμα , θα πρέπει κάποιο μέτρο να επανεξετάζεται ή αν δεν είναι από μόνο του αρκετό, να προστίθεται και κάποιο άλλο.

3) Στο τρίτο στάδιο, καταγράφεται η ασφάλεια της επεξεργασίας. Δηλαδή εκπονείται η εκτίμηση των κινδύνων (άρθρο 32), που σχετίζονται με την ασφάλεια των δεδομένων και την προάσπιση των δικαιωμάτων και ελευθεριών των υποκειμένων.

a) Προηγείται η αξιολόγηση των ήδη υλοποιημένων ή προγραμματισμένων ελέγχων και μέτρων, οι οποίοι μπορούν να λάβουν τρεις διαστάσεις:

i) μέτρα που αφορούν αποκλειστικά στα υπό επεξεργασία προσωπικά δεδομένα, όπως η κρυπτογράφηση, η ανωνυμοποίηση, η ψευδωνυμοποίηση, ο έλεγχος πρόσβασης, η ανιχνευσιμότητα, ο διαμοιρασμός κ.ά.

Ως προς την κρυπτογράφηση: θα πρέπει να εκτελείται εκτενής περιγραφή των μέσων διασφάλισης της εμπιστευτικότητας και ακεραιότητας των αποθηκευμένων δεδομένων (στη βάση αποθήκευσης, σε απλά αρχεία, σε αντίγραφα ασφαλείας κ.ά. καθώς και της διαδικασίας διαχείρισης των κλειδιών κρυπτογράφησης (δημιουργία, αποθήκευση, αλλαγή σε περίπτωση ύποπτης περίπτωσης συνδυασμού δεδομένων ή παραβίασης αυτών). Επίσης θα πρέπει να καταγραφούν τα μέτρα κρυπτογράφησης που εφαρμόζονται κατά τη ροή των δεδομένων (π.χ https, VPN). Είναι αυτά τα μέτρα αποδεκτά; Μπορούν να βελτιωθούν; Με ποιον τρόπο ή ποιο πρόσθετο μέτρο;

Ως προς την ψευδωνυμοποίηση: εφαρμόζεται; Πότε; Με ποιον τρόπο και ποιο σκοπό εξυπηρετεί; Σε ποια δεδομένα αφορά;

Ως προς τον έλεγχο πρόσβασης: τα προφίλ των χρηστών θα πρέπει να συγκεκριμενοποιούνται και να αποδίδονται στον συγκεκριμένο χρήστη. Για το λόγο αυτό θα πρέπει να οριστούν μέτρα ελέγχου της ταυτότητας (κωδικοί πρόσβασης, με ελάχιστο μήκος και απαιτούμενους χαρακτήρες, διάρκεια ισχύος, αριθμό αποτυχημένων προσπαθειών εισόδου πριν κλειδωθεί ο λογαριασμός με παράλληλη ειδοποίηση του χρήστη μέσω e-mail για απόπειρα μη εξουσιοδοτημένης εισόδου κ.ά).

Ως προς την ανιχνευσιμότητα : καταγράφονται τα ίχνη του χρήστη και για πόσο καιρό αυτά διατηρούνται, η ύπαρξη τυχόν μηχανισμών για την παρακολούθηση της ακεραιότητας των αποθηκευμένων δεδομένων, ή των ροών δεδομένων ,ποιοι είναι αυτοί;

Επίσης, θα πρέπει να καταγραφούν διαδικασίες και μέτρα που αφορούν στην ασφάλεια εγγράφων (εφόσον βέβαια υπάρχουν και έγγραφα με προσωπικά δεδομένα κατά την επεξεργασία), δηλαδή, πώς εκτυπώνονται, αποθηκεύονται καταστρέφονται ή τροποποιούνται;

ii) γενικά μέτρα ασφαλείας που αφορούν στο σύστημα στο οποίο εκτελείται η επεξεργασία, π.χ ασφάλεια λειτουργίας, αντίγραφα ασφαλείας, διαχείριση των σταθμών εργασίας, ασφάλεια του υλικού (hardware), ασφάλεια λογισμικού (software updates, antivirus software που απαιτείται), ασφάλεια καναλιών δικτύου (απομονωμένο, ιδιωτικό, Internet, τι σύστημα firewall απαιτείται, συστήματα ανίχνευσης εισβολών, ποιες και τι είδους συσκευές είναι υπεύθυνες για την εξασφάλιση της ασφάλειας του δικτύου) ή/και ιστοσελίδας, συντήρηση, έλεγχος φυσικής πρόσβασης (πώς διενεργείται ο φυσικός έλεγχος πρόσβασης στις εγκαταστάσεις που εξυπηρετούν την επεξεργασία– χωροθέτηση, συνοδεία, κλειδωμένες

πόρτες), αποφυγή πηγών κινδύνου και προστασία από αυτές (πλην του ανθρώπινου παράγοντα) και

iii) μέτρα διακυβέρνησης και οργανωτικών ελέγχων, όπως η πολιτική ασφαλείας του οργανισμού, η διαχείριση του προσωπικού, η ενημέρωση και ευαισθητοποίηση του προσωπικού του οργανισμού ως προς την ιδιωτικότητα, η διαχείριση του έργου, διαχείριση των συμβάντων και των παραβιάσεων, οι σχέσεις με τα τρίτα μέρη (εκτελούντες την επεξεργασία, σε ποια δεδομένα θα έχουν πρόσβαση και πώς θα ελέγχεται αυτή), η εποπτεία (πώς δηλαδή παρακολουθείται και ελέγχεται η επάρκεια των ελέγχων απορρήτου κ.ά[236]

b) Έπεται εν κατακλείδι, η εκτίμηση των κινδύνων σε σχέση με τις ενδεχόμενες παραβιάσεις της ιδιωτικής ζωής:

i) για κάθε ενδεχόμενο σενάριο κινδύνου- απειλής (παράνομη πρόσβαση σε προσωπικά δεδομένα– προσβολή της εμπιστευτικότητας, ανεπιθύμητη αλλαγή/τροποποίησή τους, προσβολή της ακεραιότητας, διαγραφή/εξαφάνισή τους– προσβολή διαθεσιμότητας κ.ά),πρέπει:

- να προσδιοριστούν οι επιπτώσεις στα δικαιώματα και τις ελευθερίες των υποκειμένων (να απαντηθεί το ερώτημα : “τι φοβόμαστε ότι θα προκύψει – τι συνεπάγεται η παραβίαση για τα υποκείμενα των δεδομένων;”) ,
- να εκτιμηθεί η “σοβαρότητα“ του κινδύνου, ιδίως σε σχέση με τον επιζήμιο χαρακτήρα των δυνητικών επιπτώσεων και ενδεχομένως, τα μέτρα που πιθανολογείται ότι θα τους αποτρέψουν ή μειώσουν,
- να εντοπισθούν οι “απειλές” από τα στοιχεία του ενεργητικού της επεξεργασίας για τα προσωπικά δεδομένα, που ενδεχομένως θα μπορούσαν να οδηγήσουν σε παραβίαση των δεδομένων και επίσης να ληφθούν υπόψιν οι πηγές του κινδύνου (π.χ να δοθεί απάντηση στο ερώτημα: “πώς μπορεί να συμβεί αυτό;”[237])

ii) ανάλογα με το πόσο ευάλωτα εμφανίζονται τα μέσα υποστήριξης προσωπικών δεδομένων, το επίπεδο ικανότητας των πηγών του κινδύνου να εκμεταλλευτούν αυτές τις τρωτότητες και τους ελέγχους/ μέτρα που θα μπορούσαν να τους μεταρρυθμίσουν, θα πρέπει να εκτιμηθεί η

236βλ περισσότερα για το έγγραφο πολιτικής ασφαλείας , σχέδιο ασφαλείας και σχέδιο ανάκαμψης από καταστροφές, διαθέσιμο στην ηλ δ/νση : http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/9B2485E1D6829E8FC225820A003F5E7C/$file/%CE%9F%CE%B4%CE%B7%CE%B3%CE%AF%CE%B5%CF%82%20%CF%80%CE%BF%CE%BB%CE%B9%CF%84%CE%B9%CE%BA%CE%AE%CF%82%20%CE%B1%CF%83%CF%86%CE%B1%CE%BB%CE%B5%CE%AF%CE%B

237Πηγές του κινδύνου μπορούν να αποτελέσουν εσωτερικές ανθρώπινες ενέργειες (υπάλληλοι, IT, εκπαιδευόμενοι), εξωτερικές ανθρώπινες ενέργειες (παραλήπτες, εξουσιοδοτημένοι τρίτοι, πάροχοι υπηρεσιών, hacker, ανταγωνιστές, πελάτες κ.ά) αλλά και όχι ανθρώπινες πηγές–ενέργειες (κακόβουλος κώδικας άγνωστης προέλευσης, ιοί, warms, ή και φυσικές πηγές, νερό, φυσικές καταστροφές κ.ά)

"πιθανότητα"[238].

Τέλος, θα πρέπει να καθοριστεί εάν οι κίνδυνοι που προσδιορίζονται με τον ως άνω τρόπο, μπορούν να θεωρηθούν αποδεκτοί σε σχέση με τα υφιστάμενα μέτρα και ελέγχους. Αν όχι, απαιτείται επαναξιολόγηση και επανεκτίμηση στο κάθε επίπεδο κινδύνου, ώστε να αναγνωριστούν τυχόν υπολειπόμενοι και να ληφθούν επιπλέον μέτρα ή να ζητηθεί η γνώμη της αρμόδιας Αρχής, αν δεν είναι εφικτή η λήψη κατάλληλων μέτρων ασφαλείας για τη μείωσή τους.

4) Μετά από καταγραφή όλων των ανωτέρω, η DPIA θα πρέπει να αξιολογηθεί και να επικυρωθεί, από τον υπεύθυνο επεξεργασίας (και ανά περίπτωση με τη βοήθεια του Υπεύθυνου Προστασίας των Δεδομένων). Σε αυτό το τελειωτικό στάδιο, είναι χρήσιμη η οπτική παρουσίαση των μέτρων που θα ληφθούν, η οπτική χαρτογράφηση των κινδύνων που ελλοχεύουν και φυσικά του σχεδίου αντιμετώπισης με βάση τα πρόσθετα μέτρα που τυχόν απαιτούνται. Για κάθε επιπλέον μέτρο θα πρέπει να καταγράφεται ποιος είναι υπεύθυνος για την υλοποίησή του (το κόστος του, το χρονοδιάγραμμα παράδοσής του). Επίσης, θα πρέπει να καταγράφονται οι συμβουλές του υπεύθυνου επεξεργασίας και – εφόσον έχει ζητηθεί – η άποψη των υποκειμένων των δεδομένων.

   Τέλος, η PDIA ολοκληρώνεται με την τυπική επικύρωσή της. Εδώ καταγράφονται όλα τα συμπεράσματα που προκύπτουν από την ανάλυση των προηγούμενων βημάτων. Πρακτικά αιτιολογείται εάν τα επιλεγμένα μέτρα και έλεγχοι , οι τυχόν υπολειπόμενοι κίνδυνοι και το σχέδιο αντιμετώπισης– δράσης είναι αποδεκτά , από την οπτική γωνία των εμπλεκόμενων μερών. Έτσι η DPIA, μπορεί να επικυρωθεί ή να χρειαστεί βελτίωση (αιτιολογημένη πάντα) ή να απορριφθεί (μαζί προφανώς με την υπό εξέταση επεξεργασία). Σε τέτοια περίπτωση θα πρέπει να επαναξιολογηθούν προηγούμενα βήματα ή να ζητηθεί η γνώμη της αρμόδιας Αρχής.

238Η "πιθανότητα – likelihood", μπορεί να μετρηθεί- αξιολογηθεί με βάση την ακόλουθη κλίμακα: **1.-**"***Αμελητέα***" : δεν φαίνεται πιθανό οι επιλεγμένες πηγές κινδύνου να υλοποιήσουν την απειλή λ.χ, κλοπή εγγράφων αποθηκευμένα σε μία αίθουσα που προστατεύεται με κωδικό πρόσβασης και αναγνωριστικό σήμα εισόδου), **2.-**"***Περιορισμένη***" : φαίνεται δύσκολο, οι επιλεγμένες πηγές κινδύνου να υλοποιήσουν την απειλή (π.χ. στο ως άνω παράδειγμα η πόρτα εισόδου προστατεύεται μόνο με αναγνωριστικό σήμα εισόδου), **3.-** "***Σημαντική***" : φαίνεται πιθανό οι επιλεγμένες πηγές κινδύνου να υλοποιήσουν την απειλή εκμεταλλευόμενες τις τρωτότητες ή τα υποστηρικτικά στοιχεία του ενεργητικού (π.χ κλοπή εγγράφων από γραφείο, η είσοδος στο οποίο επιτρέπεται μετά από έλεγχο στη ρεσεψιόν) και **4.- "*Μέγιστη*"** : φαίνεται εξαιρετικά εύκολο οι επιλεγμένες πηγές κινδύνου να υλοποιήσουν την απειλή (κλοπή εγγράφων αποθηκευμένων σε ερμάριο σε χώρο στον οποίο επιτρέπεται σε όλους η είσοδος) // βλ. περισσότερα CNIL, PIA Knowledge bases, Febuary 2018, σελ 11, διαθέσιμη στην ηλ δ/νση https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf

4.2.4 Γενικά σχόλια

Η διενέργεια DPIA, αποτελεί ένα καινοτόμο μέτρο που εισάγει ο νέος Κανονισμός, πλήρως εναρμονισμένο με την ανάγκη προστασίας των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού (Privacy by design / Privacy by default – αρ. 25 Κανονισμού), με το οποίο, σε συνδυασμό με την υποχρέωση του υπεύθυνου επεξεργασίας για τήρηση αρχείου δραστηριοτήτων επεξεργασίας, αντικαθιστά καταρχήν την υποχρέωση γνωστοποίησης στην ΑΠΔΠΧ της επεξεργασίας[239], όπως προβλεπόταν παλιότερα στην Οδηγία 95/46/ΕΚ και στο ν. 2472/1997. Είναι μία διαρκής διαδικασία εμπέδωσης και απόδειξης στη συμμόρφωση με τον Κανονισμό, αφού αποτελεί σημαντικό εργαλείο για την πλήρωση της αρχής λογοδοσίας, καθώς παρέχει συνδρομή στους υπεύθυνους επεξεργασίας όχι μόνον προκειμένου να συμμορφώνονται με τις προδιαγραφές του Κανονισμού, αλλά και για να αποδεικνύουν ότι έχουν ληφθεί τα ενδεδειγμένα μέτρα για τη διασφάλιση της συμμόρφωσης προς αυτόν (βλ. Άρθρο 24)[240]. Η ΑΠΔΠΧ θεωρεί ότι ερμηνευτικά η εν λόγω υποχρέωση προκύπτει και από την Οδηγία 95/46/ΕΚ και από το Ν. 2472/1997 που την ενσωμάτωσε στην ελληνική έννομη τάξη[241]. Αποτελεί ένα εργαλείο διαχείρισης των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων και, επομένως, υιοθετεί τη δική τους οπτική, όπως ισχύει σε ορισμένους τομείς (π.χ. κοινωνική ασφάλεια). Αντιθέτως, σε άλλους τομείς η διαχείριση των κινδύνων (π.χ. ασφάλεια πληροφοριών) επικεντρώνεται στην οργανωτική διάρθρωση.

Από τη διενέργεια και ολοκλήρωση της DPIA προκύπτουν πολλά σημαντικά οφέλη. Καταρχάς συμβάλλει στη διαχείριση των κινδύνων (αναγνώριση και περιορισμός/αποτροπή) με τη λήψη των κατάλληλων τεχνικών και οργανωτικών (εντός του οργανισμού) μέτρων. Έτσι επιτυγχάνεται η βελτίωση του τρόπου διαχείρισης, της προστασίας αλλά και της ποιότητας (ελαχιστοποίηση, ακρίβεια) των

239 Η αιτιολογική σκέψη 89 του Γενικού Κανονισμού αναφέρει ότι η Οδηγία 95/46/ΕΚ προβλέπει γενική υποχρέωση κοινοποίησης της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στις εποπτικές αρχές, δημιουργώντας διοικητικές και οικονομικές επιβαρύνσεις σε όλες τις περιπτώσεις χωρίς ωστόσο να συμβάλει ουσιαστικά στη βελτίωση της προστασίας των δεδομένων αυτών. Επομένως, η ως άνω γενική υποχρέωση κοινοποίησης χωρίς διακρίσεις θα πρέπει να καταργηθεί και αντικατασταθεί από αποτελεσματικές διαδικασίες και μηχανισμούς, οι οποίοι επικεντρώνονται αντ' αυτού σε εκείνους τους τύπους επεξεργασίας που ενδέχεται να οδηγήσουν σε υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων λόγω της φύσης τους, το πλαίσιο και τους σκοπούς τους. Διαθέσιμη στην ηλ. διεύθυνση https://gdpr-info.eu/recitals/no-89/.

240 Βλ. επίσης αιτιολογική σκέψη 84: «Το αποτέλεσμα της εκτίμησης θα πρέπει να λαμβάνεται υπόψη όταν καθορίζεται ποια μέτρα ενδείκνυται να ληφθούν ώστε να αποδειχθεί ότι η επεξεργασία των δεδομένων προσωπικού χαρακτήρα είναι σύμφωνη με τον παρόντα κανονισμό».

241 Βλ. πρόσφατη Γνωμοδότηση της ΑΠΔΠΧ 1/2017 σχετικά με τη γνωστοποίηση επεξεργασίας προσωπικών δεδομένων στο πλαίσιο του Ηλεκτρονικού Εισιτηρίου του ΟΑΣΑ, ιδίως τις Σκέψεις υπ' αρ. (3) επ., διαθέσιμη στην ηλ. δ/νση http://www.dpa.gr/portal/page?_pageid=33,120923&_dad=portal& και Δημήτρης Γ. Ζαφειρόπουλος, Ειδικός Επιστήμονας στην ΑΠΔΠΧ, άρθρο "Η υποχρέωση διενέργειας εκτίμησης αντικτύπου στον Γενικό Κανονισμό για την Προστασία Δεδομένων " - διαθέσιμο στην ηλ. δ/νση http://files.cyberinsurancequote.webnode.com/200000185-c1077c2000/THEMA_ZOGRAFOPOULOS.pdf.

δεδομένων. Η έγκαιρη κατανόηση και καταγραφή των κινδύνων που ελλοχεύει ένα έργο, συνεπάγεται αφενός την πρόληψη της διακοπής του, αφετέρου την αποτροπή δαπανηρών και κοστοβόρων προσαρμογών σε μετέπειτα επεξεργασίες ή επανασχεδιασμό ενός συστήματος, αφού ο στόχος παραμένει από την αρχή μέχρι το τέλος ο ίδιος: η προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων. Επίσης, η διενέργεια DPIA βελτιώνει τις διαδικασίες εξυπηρέτησης των υποκειμένων και λειτουργίας, με αποτέλεσμα την ενίσχυση της εμπιστοσύνης των υποκειμένων ως προς τον τρόπο επεξεργασίας των δεδομένων αλλά και την ευαισθητοποίηση των εργαζομένων και εν γένει εμπλεκόμενων μερών ως προς την προστασία της ιδιωτικής ζωής. Τέλος, αποδεικνύει τη συμμόρφωση με τη νομοθεσία για την προστασία των δεδομένων και μειώνει την πιθανότητα επιβολής κυρώσεων[242].

Έπειτα από τα ανωτέρω, γίνεται εμφανές ότι υπό τις προϋποθέσεις του άρθρου 35, ο πελάτης υπηρεσιών νεφοϋπολογιστικής, δέον όπως προβεί στη διενέργεια DPIA, πόσο μάλλον αφού το περιβάλλον του cloud computing αποτελεί μία νέα τεχνολογία που “επεξεργάζεται” τουλάχιστον μεγάλου όγκου δεδομένα, που λόγω της πολυπλοκότητας της αρχιτεκτονικής της βρίσκεται μονίμως υπό απειλή. Από την άλλη και οι πάροχοι υπηρεσιών νέφους, εφόσον έχουν την ιδιότητα του υπεύθυνου επεξεργασίας, καλούνται να διενεργήσουν την DPIA [243].

5 Επίλογος

Η αλματώδης πρόοδος και συνεχής εξέλιξη της τεχνολογίας του cloud computing (με τις τεχνολογίες που αυτό ενσωματώνει : big data, IoT) συμβάλλει στην βελτίωση της καθημερινής ζωής. Το cloud copmuting είναι το περιβάλλον εργασίας της πληροφορικής του μέλλοντος, με εμβέλεια και βάσεις σε όλο τον κόσμο. Ταυτόχρονα όμως, εισβάλει όλο και περισσότερο στη σφαίρα της ιδιωτικής ζωής, και των προσωπικών δεδομένων των χρηστών του, αφού η ολοένα αναπτυσσόμενη συλλογή προσωπικών δεδομένων και ανταλλαγή τους μέσω νέφους, δημιουργεί πολλά προβλήματα σχετικά με την προστασία τους. Οι κίνδυνοι που προσιδιάζουν στο υπολογιστικό νέφος για τα προσωπικά δεδομένα, σχετίζονται με την ίδια του τη φύση και την αρχιτεκτονική του.

242 Smart Grid Task Force 2012-14 Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems, διαθέσιμο στην ηλ δ/νση : https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

243 Όπως προαναφέρθηκε, ένα διεθνές πρότυπο το οποίο παρέχει κατευθυντήριες γραμμές για τις μεθοδολογίες που χρησιμοποιούνται στη διενέργεια DPIA στους παρόχους είναι το ISO/IEC 29134 (έργο), *Τεχνολογία Πληροφοριών – Τεχνικές Ασφαλείας – Εκτίμηση επιπτώσεων στην ιδιωτικότητα – Οδηγίες*, Διεθνής Οργανισμός Τυποποίησης (ISO), για περισσότερες πληροφορίες βλ ηλ δ/νση : https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

Σύμφωνα με τη Συμμαχία Ασφάλειας Cloud (Cloud Security Alliance), οι τρεις πρώτες απειλές στο υπολογιστικό νέφος είναι οι ασφαλείς διεπαφές και οι Διεπαφές Προγραμματισμού Εφαρμογών (Application Programming Interface – API), η απώλεια δεδομένων, καθώς και η διαρροή και αποτυχία υλικού, που αντιστοιχούν σε 29%, 25% και 10% όλων των διακοπών ασφαλείας του cloud αντίστοιχα.

Ο νέος Κανονισμός 2016/679 (ΕΕ), θεσπίζει ένα ισχυρό νομικό και θεσμικό πλέγμα προστασίας των προσωπικών δεδομένων, με ομοιόμορφη εφαρμογή εντός Ε.Ε. αλλά και εκτός αυτής, ενισχύοντας τα δικαιώματα των υποκειμένων και αυξάνοντας παράλληλα τις υποχρεώσεις του υπεύθυνου επεξεργασίας και εκτελούντος αυτήν. Στόχος του είναι η αντιμετώπιση των προβλημάτων που δημιουργεί η χρήση των νέων τεχνολογιών πληροφορικής, όπως αυτή του cloud computing.

Ωστόσο, η συμμόρφωση με αυτόν, ειδικά για τους παρόχους υπηρεσιών νέφους, απαιτεί μεγάλες οικονομικές επενδύσεις, για την ανάπτυξη ενός κοινού προτύπου διαλειτουργικού περιβάλλοντος αλλά και νέων τεχνικών μέτρων για την προστασία των δεδομένων, που θα καθορίζουν την πρόσβαση και διαχείριση των χρηστών, τις τεχνικές ασφαλείας, τον τρόπο ανάκτησης αλλά και διαγραφής των δεδομένων, μέτρα που προς το παρόν μόνο μεγάλοι οικονομικά πάροχοι είναι σε θέση να υλοποιήσουν. Επίσης, θα πρέπει να καθοριστεί ένα συγκεκριμένο πλαίσιο (νομικό και τεχνικό) βάση του οποίου θα αξιολογούνται οι SLAs. Συνάμα, επιτακτική φαντάζει η ευελιξία στην κατάρτιση των Συμβάσεων Παροχής Νέφους (Cloud Provisioning Contract), και δη από τους παρόχους υπηρεσιών νέφους, σε αντίθεση με τη σημερινή πραγματικότητα των προδιατυπωμένων όρων, ώστε να επιτευχθεί η διαφάνεια, η λογοδοσία, η πραγματική ασφάλεια και κατανομή των ευθυνών.

Τέλος, οι αρμόδιες εποπτικές ευρωπαϊκές αρχές θα πρέπει να καταλήξουν στην υιοθέτηση κοινών προτύπων πιστοποίησης, ασφάλειας και εταιρικών δεσμευτικών κανόνων, για να βοηθήσουν παρόχους και πελάτες υπολογιστικής νέφους στην άρτια συμμόρφωση με τον Κανονισμό και την ασφαλή διαβίβαση δεδομένων σε τρίτες χώρες.

Κλείνοντας, θα πρέπει να διερευνηθούν τα “κενά” που δημιουργεί ο Νέος Κανονισμός 2016/679 (ΕΕ), όπως ήδη τονίζει και η Ομάδα του άρθρου 29 και δη σε σχέση με τις επί μέρους νομοθετικές ρυθμίσεις που έχει ή θα υιοθετήσει έκαστο Κράτος–Μέλος της Ένωσης, με στόχο να φωτιστούν οι “γκρίζες ζώνες” που δημιουργεί η εφαρμογή του, ειδικά στο περιβάλλον του νέφους. Δυστυχώς, παρόλο που ο Κανονισμός 2016/679 (ΕΕ) τέθηκε σε ισχύ ήδη από τον Μάιο, στη χώρα μας ακόμη, ούτε έχει ψηφισθεί ο Νόμος, που ρυθμίζει τα ειδικότερα θέματα σε συμμόρφωσή του, ούτε οι χρήστες των υπηρεσιών νέφους έχουν αντιληφθεί τις

διαδικασίες στις οποίες πρέπει να προβούν για τη συμμόρφωσή τους με αυτόν.

ΧΡΗΣΙΜΟΙ ΣΥΝΔΕΣΜΟΙ:

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679

https://gdpr-info.eu/

https://www.nist.gov/

http://www.dpa.gr/

http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument

https://www.cnil.fr/

https://ico.org.uk/

https://europa.eu/european-union/index_el

https://ec.europa.eu/commission/index_en

https://curia.europa.eu/jcms/jcms/j_6/el/

https://www.enisa.europa.eu/

https://www.iso.org/home.html

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνική :

- *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Προσωπικά Δεδομένα, Νομική Βιβλιοθήκη (2016)
- *Ιωάννης Ιγγλεζάκης*, Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, εκδ. Interactive, 2018
- *Ιωάννης Δ. Ιγγλεζάκης* , Το δικαίωμα στην ψηφιακή λήθη και οι περιορισμοί του, εκδόσεις Σάκκουλα 2014
- *Μήτρου Λίλιαν,* Ο Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων, Νέο Δίκαιο, Νέες Υποχρεώσεις, Νέα Δικαιώματα, Εκδόσεις Σάκκουλα, Α.Ε. 2017
- *Παναγοπούλου – Κουτνατζη* Φ., *Ο Γενικός Κανονισμός για την προστασία Δεδομένων 679/2016, Εκδόσεις Σάκκουλα 2017*
- *Παναγοπούλου – Κουτνατζή Φ., Η εξέλιξη του δικαιώματος στη λήθη (περί λήθης της λήθης;), ΕφημΔΔ 2016.714-728*
- *Παναγοπούλου-Κουτνατζή Φ., Περί της προσωπικής - οικιακής χρήσεως των προσωπικών δεδομένων, ΕφΔΔ 2013.704-718,*
- *Σμυρνάκη Ευγενία , Υπ. Διδάκτωρ Νομικής Σχολής ΑΠΘ, Υπολογιστικό Νέφος (Cloud) και Προσωπικά Δεδομένα - Γενικός Κανονισμός Προστασίας Δεδομένων 679/2016*
- *Σωτηρόπουλος Βασίλης, Υπεύθυνος Προστασίας Δεδομένων, εργαλειοθήκη για το νέο θεσμό σε δημόσιο και ιδιωτικό φορέα, εκδόσεις Σάκκουλα 2017* ,
- *Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων*, Γνώμη 3/2010 σχετικά με την αρχή της λογοδοσίας (13-7-2010)
- *Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων*, Γνώμη 2/2009 για την προστασία προσωπικών δεδομένων παιδιών (γενικές κατευθυντήριες γραμμές και η ειδική περίπτωση των σχολείων) (11-2-2009)
- *Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων* , WP 248, Κατευθυντήριες γραμμές για την εκτίμηση του αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) και καθορισμός του κατά πόσον η επεξεργασία «ενδέχεται να επιφέρει υψηλό κίνδυνο» για τους σκοπούς του κανονισμού 2016/679 , που εκδόθηκαν την 04.04.2017, όπως τελικά αναθεωρήθηκαν και

εκδόθηκαν την 4 Οκτωβρίου 2017

- Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων, Γνώμη 1/2010 σχετικά με τις έννοιες του «υπεύθυνου επεξεργασίας» και του «εκτελούντος την επεξεργασία»
- *Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων*, Γνώμη 4/2007 σχετικά με την έννοια του όρου προσωπικά δεδομένα , της 20ης Ιουνίου 2007
- *Ομάδα εργασίας του άρθρου 29 για την προστασία των δεδομένων,* Γνώμη 05/2012 σχετικά με τη νεφοϋπολογιστική , της 1ης Ιουλίου 2012

Ξενόγλωσση :

- *Article 29 Data Protection Working Party*, Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing, Adopted on 22 September 2015,
- *Article 29 Data Protection Working Party*, Guidelines on Personal data breach notification under Regulation 2016/679, adopted on 3 October 2017
- *Article 29 Data Protection Working Party*, Guidelines on Data Protection Officers ('DPOs')
- *Article 29 Data Protection Working Party*, Guidelines on the right to data portability, adopted on 13 December 2016, όπως αναθεωρήθηκε και υιοθετήθηκε στις 5 Απριλίου 2017
- *Article 29 Data Protection Working Party*, Guidelines on the application and setting administrative fines for the purposes of the Regulation 2016/697, adopted on 3 October 2017
- *Article 29 Data Protection Working Party*, Guidelines on consent under Regulation 2016/679 , adopted on 28 November 2017, as last revised and adopted on 10 April 2018
- *Bitcom, Risk Assessment & Data Protection Impact Assessment , Guide*
- *Bob Duncan, University of Aberdeen, UK YongWoo Lee,* University of Seoul, Korea Aspen Olmsted, College of Charleston, USA, **"**CLOUD COMPUTING 201"8, The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization ISBN: 978-1-61208-607-1 February 18 - 22, 2018 Barcelona, Spain CLOUD COMPUTING 2018 ,
- *CNIL, PIA, Knowledge bas, Febuary 2018*
- *CNIL, Privacy Impact Assessment (PIA) METHODOLOGY, Feb 2018*
- *CNIL, Privacy Impact Assessment (PIA) TEMPLATES, Febuary 2018*

- *CNIL, Recommendations for companies planning to use Cloud computing services*
- *ENISA*, Cloud Computing Risk Assessment, December 2012
- *ENISA* Privacy and Data Protection by Design - from policy to engineering –December 2014
- *ENISA* , Certification in the EU Cloud Strategy
- *ENISA* , Critical Cloud Computing, A CIIP perspective on cpoud cpmouting services, Version 1,0, December 2012
- *ENISA)*, Privacy and Data Protection by Design – from policy to engineering (Δεκέμβριος 2014),
- *ENISA, Guidelines for SMEs on ths security of personal data processing*
- *Fang Liu, Jin Tong, Jian Mao, Robert Bohn, John Messina, Lee Badger and Dawn Leaf , NIST, Cloud Computing Reference Architecture Recommendations of the National Institute of Standards and Technology , Special Publication 500-292*
- *Hoboken JVJ, The Proposed Right to be Forgotten Seen from the Perspective of Our Right to Remember, Freedom of Expression Safeguards in a Converging Information Environment (Ιούνιος 2013)*
- *KEITH MARTIN, "Everyday Cryptography, Fundamental Principles & Applications", OXFORD,*
- *KUROSE/ ROSS, Compruter Networking, A Top-Down Approach, sixth edition,*
- *Thomas Erl, Cloud Computing, Αρχές Τεχνολογία & Αρχιτεκτονική, εκδόσεις Μ. Γκιούρδας*

άρθρα :

- *Αλεξανδροπούλου-Αιγυπτιάδου Ε.*, Κοινωνία της πληροφορίας και νομική προστασία των προσωπικών δεδομένων της οικογένειας και των μελών της, ΕλλΔνη 2008.691-699
- *Κομνηνός Γ. Κόμνιος*, Οι γενικοί όροι επιβολή διοικητικών προστίμων κατά τον Γενικό Κανονισμό για την Προστασία των Δεδομένων, Συμβολή στην ερμηνεία του άρθρου 83 του γενικού Κανονισμού για την Προστασία των Δεδομένων, ΔΙΜΕΕ τ. 4/2017
- *Π. Κίτσος - Π. Παππά*, Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στις υπηρεσίες του υπολογιστικού νέφους, ΔΙΜΕΕ 2/2012

- *Παναγιώτης Παπαδημητρίου*, *Privacy Aspects for Cloud Computing,* Department of Allpied Informatics , University of Macedonia, Greece ,
- *Bob Ducan* , "Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing", CLOUD COMPUTING 2018, The Ninth Conference on Cloud Computing , GRIDs, and Virtualization
- *Bob Duncan*, John D. Lamb, Ndubuisi Anomelechi, William Cooper, "A Management View of Security and Cloud Computing", CLOUD COMPUTING 2018 : The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization,
- *Christos Stergiou a, Kostas E. Psannis a,⁎, Byung-Gyu Kimb, Brij Guptac* **"**Secure integration of IoT and Cloud Computing ",
- *El Balmany Chawkia , Asimi Ahmeda , Tbatou Zakariaea*, "The 2nd International Workshop on Big Data and Networks Technologies (BDNT'2018) IaaS Cloud Model Security Issues on Behalf Cloud Provider and User Security Behaviors "
- *HASSAN TAKABI and JAMES B.D.* , "Security and Privacy Challenges in Cloud Computing Environments", 2010
- *Justice Opara-Martins, Reza Sahandi and Feng Tian*, "Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective", 2016
- *Mark Webber*, "The GDPR's impact on the cloud computing service provider as a processor", Privacy & Data Protection, VOLUME 16, ISSUE 4
- *Marina Škrinjar Vidović**, EU DATA PROTECTION REFORM: CHALLENGES FOR CLOUD COMPUTING
- *Massino Maggiore*, "EU, Cloud Computing: obligations under thw Directive v. GDPR", June 2016
- *Mitrou L./Karyda M.*, EU's Data Protection Reform and the Right to be Forgotten: A Legal Response to a Technological Challenge? (February 5, 2012), 5th International Conference of Information Law and Ethics 2012, Corfu-Greece, June 29-30, 2012
- *P. Ravi Kumara, P. Herbert Rajb, P. Jelcianac* , "Exploring Data Security Issues and Solutions in Cloud Computing ", The 6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India
- *Purtova N.*, Property in Personal Data: Second Life of an Old Idea in the Age of Cloud

Computing, Chain Informatisation, and Ambient Intelligence (July 16, 2010). TILT Law & Technology Working Paper No. 2010/017

- *Reginaldo Rea,, Romulo Manciola Melocaa, Douglas Nassif Roma Juniorb, Marcelo Alexandre da Cruz Ismaelc, Gabriel Costa Silva*, "An Empirical Study for Evaluating the Performance of Multi-cloud APIs ", Science Direct
- *Sapountzi A. – Psannis K*., Social networking data analysis tools & challenges

Stergiou C. – Psannis K., Efficient and Secure big data delivery in cloud computing