Cloud Computing και Νομικά Ζητήματα Προστασίας Προσωπικών Δεδομένων

Τάκης Κακούρης,
Partner, Ζέπος & Γιαννόπουλος

Τι είναι το Υπολογιστικό Νέφος

Αποθήκευση/επεξεργασία/ χρήση δεδομένων σε απομακρυσμένους υπολογιστές που είναι προσβάσιμοι μέσω Διαδικτύου

NIS Directive (Network and Information Systems) : «υπηρεσίες νεφοϋπολογιστικής» επιτρέπουν την πρόσβαση σε κλιμακοθετήσιμο και ελαστικό σύνολο κοινόχρηστων υπολογιστικών πόρων.

Οφέλη

- Απεριόριστη υπολογιστική ισχύς, on demand
- Χαμηλό κόστος/ όχι μεγάλες επενδύσεις κεφαλαίων
- Ελάχιστη διαχειριστική προσπάθεια (λόγω της εικονικότητας/ απουλοποίησης) για άντληση δεδομένων
- Αποδοτικότητα ειδικά για ΜΜΕ
- Ανακατανομή πόρων/προσωπικού
- Αύξηση τηλεργασίας, παραγωγικότητας, τυποποίησης
- Άρα νέες ευκαιρίες, νέες αγορές, καινοτομία, οφέλη για μικρές οικονομίες/απομακρυσμένες περιοχές
- Οφέλη και για δημόσιο τομέα αλλά αναγκαία η διάκριση πληροφοριών και επιλογή αξιόπιστων παρόχων (Εσθονία)

Κίνδυνοι για την ιδιωτικότητα

- Επαναπροσδιορίζεται το πώς, πού και από ποιον συλλέγονται, διαβιβάζονται και χρησιμοποιούνται τα δεδομένα
- Συσσώρευση μεγάλου όγκου προσωπικών δεδομένων
- Εμπορευματοποίηση προσωπικών δεδομένων;
- Απώλεια ελέγχου
  - ✓ Που αποθηκεύονται; Εντός/Εκτός ΕΕ;
  - ✓ Ποιος έχει πρόσβαση;
  - ✓ Και αν χρησιμοποιούνται και τρίτοι πάροχοι;
  - ✓ Και αν κάτι πάει «στραβά»; (cyberattack, αίτημα)
  - ✓ Πως τα ανακτώ;
  - ✓ Πως ασκώ τα δικαιώματα μου;

Διαφορές με «κλασικό» εξωπορισμό (outsourcing)

- Πάροχοι outsourcing
  - ✓ Προσφέρουν όχι μόνο υποδομή αλλά και λειτουργίες
  - ✓ Έχουν πρόσβαση στο περιεχόμενο
  - ✓ Μεγάλες εξατομικευμένες (tailored)/παραμετροποιημένες συμφωνίες
  - ✓ Πελάτης καθοδηγεί την συμφωνία (βλ. ΠΔΤΕ για outsourcing)
  - ✓ Υψηλό κόστος/ άμεση χρηματοδότηση από τον πελάτη

- Πάροχοι cloud
  - ✓ Μεγάλης κλίμακας πελατειακή βάση (μικρομεσαίες επιχ)
  - ✓ Μικρότερα ποσά
  - ✓ Κατανομή κόστους/ φθηνότερη λύση
  - ✓ Όχι capex για πελάτες/ capex για πάροχο

Νομική υπαγωγή

- Υπεύθυνος επεξεργασίας: ο πελάτης
- Εκτελών την επεξεργασία: ο πάροχος υπηρεσιών νέφους
- Έτσι και η ΑΠΔΠΧ, βλ. Ετήσιες Εκθέσεις 2015 (σ. 57) και 2012 (σ.70)
- Υπεύθυνος επεξεργασίας ο πάροχος μόνο εφόσον επεξεργάζεται δεδομένα για ίδιους ή νέους σκοπούς (marketing, διαβίβαση σε τρίτους)
- Σημαντικά κείμενα
  - ✓ WP Opinion 5/2012 (η «κορωνίδα» επί των θεμάτων)
  - ✓ WP Opinion 2/2015 on C-SIG Code of Conduct on CC
  - ✓ Και μια ιδιωτική πρωτοβουλία Cloud Privacy Check http://cloudprivacycheck.eu (ρύθμιση του CC σε 32 χώρες)
  - ✓ NIS Directive 2016/1148

Νομικές απαιτήσεις του cloud

- Προσδιορισμός σκοπού: για καθορισμένους, σαφείς και νόμιμους σκοπούς
- Περιορισμός σκοπού: Απαγόρευση χρήσης δεδομένων για άλλους (ίδιους) σκοπούς (όχι διαφήμιση/ όχι για κέρδος με βάση δεδομένα πελατών)
- Κατάλληλα τεχνικά και οργανωτικά μέτρα για ασφάλεια και εμπιστευτικότητα
- Διασφάλιση των δικαιωμάτων πρόσβασης, διόρθωσης, διαγραφής, δέσμευσης και αντίρρησης
- Πελάτης παραμένει κύριος των δεδομένων άρα
  - ✓ Επιστροφή κατά τη λήξη ή καταγγελία
  - ✓ Φορητότητα

Περιεχόμενο σύμβασης πελάτη- παρόχου (προστασία δεδομένων και όχι μόνο)

- Διαφάνεια / «ενημέρωση» του πελάτη μέσω της σύμβασης
  - ✓ Defined terms
  - ✓ Χαρακτηριστικά νέφους /τυχόν πιστοποιήσεις (ISO27018) άλλως έλεγχος
  - ✓ SLAs
  - ✓ Μέτρα ασφάλειας, ποιος έχει πρόσβαση και πότε/ update
  - ✓ Συμβάντα παραβίασης (data breach)
  - ✓ Ενημέρωση για ελέγχους
  - ✓ Χρήση «υπεργολάβων» (έγκριση ή ενημέρωση και δικαίωμα καταγγελίας του πελάτη)
  - ✓ Αντίγραφα (Backup)/ Ανάκτηση (restore)/ Φορητότητα

Περιεχόμενο σύμβασης πελάτη- παρόχου (προστασία δεδομένων και όχι μόνο)

- ✓ Κατάλογος με τοποθεσίες επεξεργασίας/κανονιστική συμμόρφωση
- ✓ Ενημέρωση για δεσμευτικά αιτήματα κοινοποίησης δεδομένων
- ✓ Εύκολη λύση σύμβασης (no vendor lock-in)
- ✓ Άλλες συμβατικές ρήτρες (περιορισμός ευθύνης)
- ✓ Αναφορά σε Κώδικες Δεοντολογίας (συμπληρωματική εφαρμογή)

Διαβιβάσεις δεδομένων

- Διαβίβαση εντός ΕΕ
- Διαβίβαση εκτός ΕΕ/διασυνοριακά νέφη
  - ✓ Άδεια της ΑΠΔΠΧ
  - ✓ Απλή γνωστοποίηση/ Όχι άδεια της ΑΠΔΠΧ όταν
    - Ικανοποιητικό επίπεδο προστασίας
    - Privacy Shield για ΗΠΑ αλλά πάντα έγγραφη σύμβαση με εκτελούντα στις ΗΠΑ
    - C2P Model clauses
- Γερμανικές Αρχές Προστασίας δεν θεωρούν επαρκές το πλαίσιο ακόμα και των Model Clauses, Schrems II
- Τάση προς clouds εντός ΕΕ (Microsoft)

Ειδικές ρυθμίσεις

- Τράπεζες (Παράρτημα 1 της ΠΔΤΕ 2577/2006)
  - ✓ Απαγόρευση για ουσιώδης/σημαντική λειτουργία
  - ✓ Μη ουσιώδης με άδεια της ΤτΕ
  - ✓ Λίστα *de minimis* /Δικαίωμα ελέγχου «επόπτη»

- Ασφαλιστικές (άρθρο 49 του ν. 4364/2016)
  - ✓ Απαγόρευση για σημαντική ή κρίσιμη λειτουργία όταν κίνδυνος σε διακυβέρνηση, λειτουργικός κίνδυνος, εποπτικός, εξυπηρέτηση ασφαλισμένων
  - ✓ Προηγούμενη ενημέρωση στην ΤτΕ

Ειδικές ρυθμίσεις /κανονιστική συμμόρφωση

- Τηλεπικοινωνιακές, εκ του νόμου τήρηση δεδομένων εντός Ελλάδος (άρθρο 6 ν. 3917/2011)

- Δημόσιος τομέας
  - ✓ όχι απαγόρευση
  - ✓ αλλά ούτε και χρήση
  - ✓ προσαρμογές στο δίκαιο προμηθειών (subscription)
  - ✓ «*όταν φορείς δημόσιας διοίκησης χρησιμοποιούν υπηρεσίες που προσφέρονται από παρόχους ψηφιακών υπηρεσιών, ιδίως υπηρεσίες cloud, μπορούν να απαιτούν πρόσθετα μέτρα ασφάλειας από τους παρόχους των υπηρεσιών αυτών, επιπλέον όσων θα προέβλεπαν κανονικά οι πάροχοι ψηφιακών υπηρεσιών. Τούτο θα πρέπει να μπορεί να γίνεται μέσω συμβατικών υποχρεώσεων*» (Σκέψη 54 NIS Directive)

Ο Νέος Κανονισμός 2016/679 (GDPR)

- Όχι ειδικές διατάξεις για το νέφος / τεχνολογική ουδετερότητα
- Γεωγραφικό πεδίο εφαρμογής Κανονισμού (εγκατάσταση ανεξάρτητα από επεξεργασία, προσφορά αγαθών/υπηρεσιών στην ΕΕ, παρακολούθηση συμπεριφοράς προσώπων στην ΕΕ)
- Άμεσες ειδικές υποχρεώσεις cloud provider
  - ✓ Έγγραφη σύμβαση (αντικείμενο, σκοπός, κατηγορίες υποκειμένων)
  - ✓ Διαβεβαιώσεις για τεχνικά/οργανωτικά μέτρα/ασφάλεια
  - ✓ Πρόσληψη άλλου εκτελούντα με άδεια υπευθύνου/ πλήρως υπόλογος ο αρχικός εκτελών
  - ✓ Ειδοποίηση σε παραβίαση
- Αναφορά σε τήρηση εγκεκριμένων κωδίκων δεοντολογίας (άρθρα 40-41)
- Αναφορά σε μηχανισμούς πιστοποίησης από ειδικούς φορείς (άρθρα 42-43)

Τα μεγάλα ζητήματα

- Εμπιστοσύνη
  - ✓ Συμμόρφωση με την ισχύουσα νομοθεσία
  - ✓ Σαφήνεια συμβατικών όρων
  - ✓ Πιστοποίηση
  - ✓ Περαιτέρω αυτορρύθμιση των παρόχων με Κώδικες Δεοντολογίας (βλ. WP 232 Opinion 2/2015 on C-SIG CoC on Cloud Computing)
  - ✓ Τυποποίηση συμβάσεων και σαφήνεια για τους χρήστες/ «υπεύθυνους»
  - ✓ Αύξηση του ελάχιστου επιπέδου προστασίας
  - ✓ NIS Directive 2016/1148 υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών

- Τελικά το Cloud ως δημόσιο αγαθό (utility)

Σας ευχαριστώ