Ο GDPR στην Ψηφιακή Τραπεζική

3RD LAW FORUM ON DATA PROTECTION & PRIVACY

22 Φεβρουαρίου 2019

Σοφία Μπίζα, Δικηγόρος LLM, Compliance & Data Protection Manager, Praxia Bank

Πρόσφατες εξελίξεις

GDPR vs PSD2

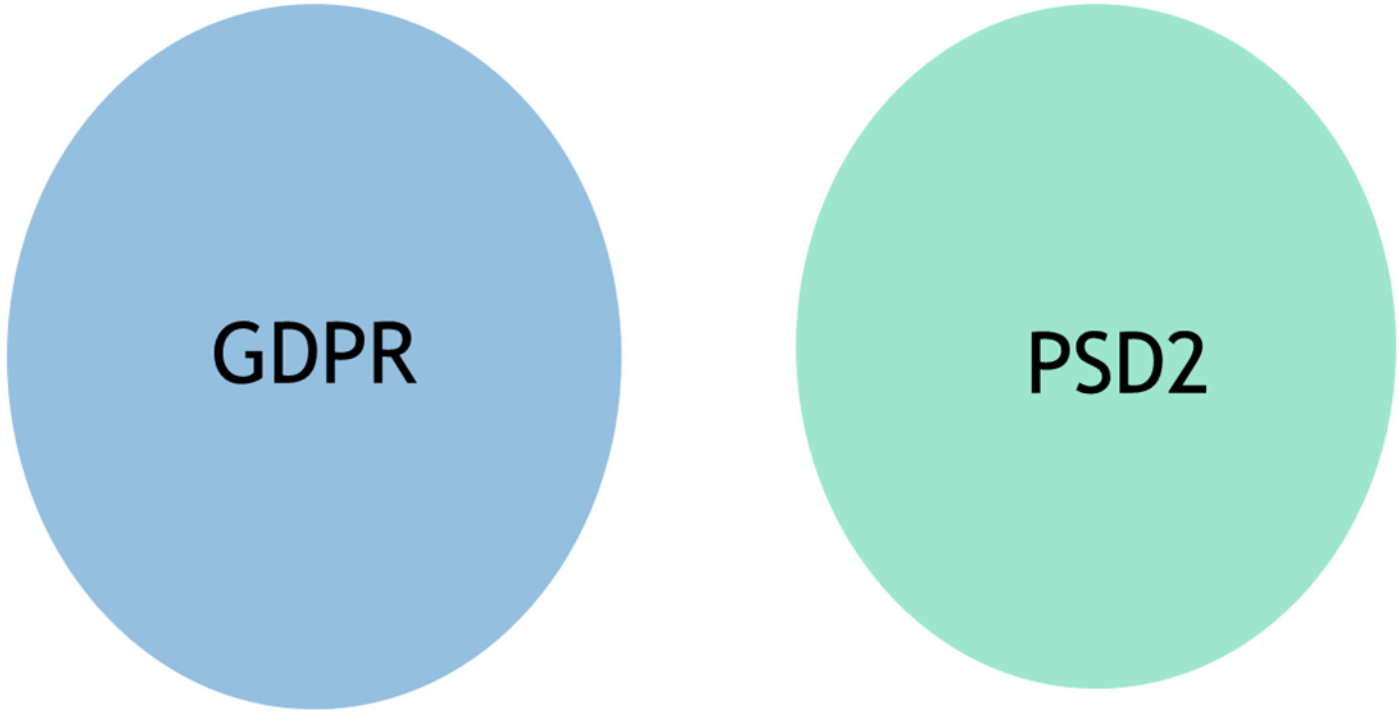
GDPR

- Προστασία προσωπικών δεδομένων φυσικών προσώπων
- Αρχές και βάσεις για τη νόμιμη επεξεργασία των προσωπικών δεδομένων
- Αυξημένα δικαιώματα των ΥΔ
- Αρχή λογοδοσίας για τους ΥΕ & ΕΕ
- Αυστηρές τεχνικές προδιαγραφές για την ασφάλεια των προσωπικών δεδομένων
- Πρόβλεψη αυστηρών κυρώσεων σε περίπτωση παραβίασης

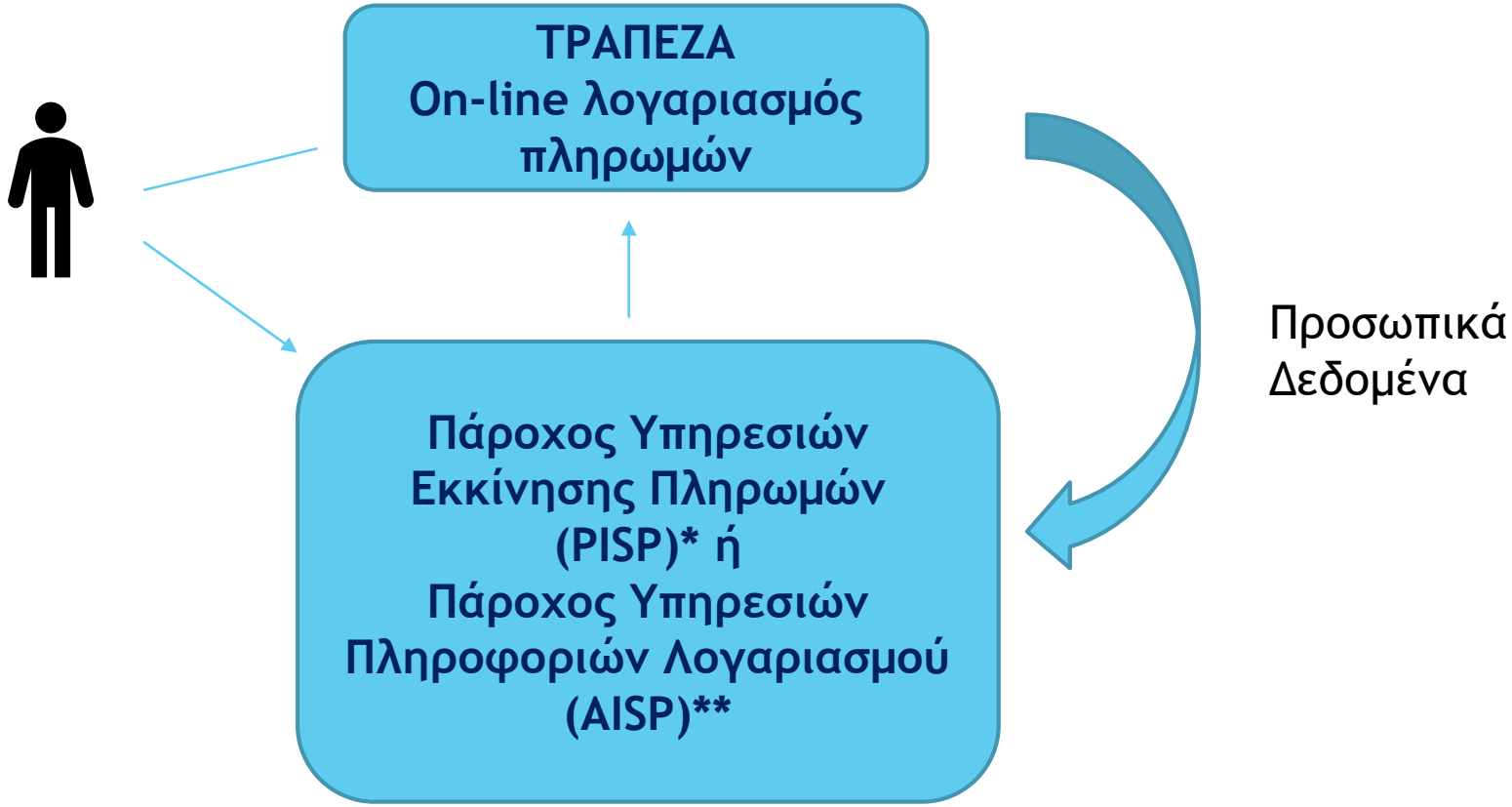
PSD2

- Αναθεώρηση νομικού πλαισίου για τις υπηρεσίες πληρωμών
- Πρόβλεψη νέων υπηρεσιών πληρωμών
- Είσοδος νέων φορέων παροχής υπηρεσιών πληρωμής (κυρίως PISPs & AISPs)
- Αυστηρές απαιτήσεις για την ασφάλεια των ηλεκτρονικών υπηρεσιών πληρωμών
- Ανοιχτή (ασφαλής) πρόσβαση σε προσωπικά δεδομένα από TPPs
- Open Banking

GDPR vs PSD2



Παράδειγμα



*PISP: απαιτείται άδεια από την ΤτΕ και καταχώριση στο δημόσιο μητρώο αυτής
**AISP: απαιτείται μόνο καταχώριση στο δημόσιο μητρώο της ΤτΕ

Ζητήματα προσωπικών δεδομένων από την εφαρμογή της PSD2

Άρθρο 93 παρ. 2 Ν. 4537/18: *Η ρητή συγκατάθεση του χρήστη υπηρεσιών πληρωμών συνιστά προϋπόθεση για την πρόσβαση, επεξεργασία και διατήρηση των δεδομένων προσωπικού χαρακτήρα που είναι αναγκαία για την παροχή υπηρεσιών πληρωμών από τους παρόχους υπηρεσιών πληρωμών.*

- Είναι η συγκατάθεση η νόμιμη βάση επεξεργασίας;
- Τι ισχύει ως προς τα δεδομένα του δικαιούχου της πληρωμής (silent party data);
- Ποιος είναι υπεύθυνος να αποδείξει ότι έλαβε τη συγκατάθεση;
- Πώς ανακαλείται η συγκατάθεση;

Ζητήματα προσωπικών δεδομένων από την εφαρμογή της PSD2

Άρθρο 4, περ. 32 Ν. 4537/2018: *«ευαίσθητα δεδομένα πληρωμών»: δεδομένα τα οποία περιλαμβάνουν και τα εξατομικευμένα διαπιστευτήρια ασφάλειας και τα οποία μπορεί να χρησιμοποιηθούν για διάπραξη απάτης. Για τις δραστηριότητες των PISPs και AISPs, το όνομα του δικαιούχου του λογαριασμού και ο αριθμός του λογαριασμού πληρωμών δεν συνιστούν ευαίσθητα δεδομένα πληρωμών.*

- Ανήκουν τα «ευαίσθητα δεδομένα πληρωμών» στις ειδικές κατηγορίες προσωπικών δεδομένων του GDPR;
- Σε ποια δεδομένα αποκτά πρόσβαση ο τρίτος πάροχος υπηρεσιών πληρωμών;
- Τι σημαίνει ανοιχτές APIs και πώς σχετίζονται με το δικαίωμα στη φορητότητα των δεδομένων;
- Η μέθοδος “screen scraping” είναι ασφαλής;

GDPR compliant?
ή
PSD2 compliant?

Ευχαριστώ