					Εισαγάγετε εδώ την επωνυμία του καταχωρισμένου νομικού προσώπου							
Αριθμός εγγράφου: PII02					Τίτλος εγγράφου: **Πολιτική ρόλων, αρμοδιοτήτων και λογοδοσίας για την ιδιωτικότητα**							
Έκδοση: 1.0		Ημερομηνία έναρξης ισχύος: 01.01.2025			Ιδιοκτήτης εγγράφου:							
X	Πολιτική		Πρότυπο		Διαδικασία		Έντυπο		Μητρώο		Άλλο	

Ιστορικό αναθεωρήσεων				
Αριθμός αναθεώρησης	**Ημερομηνία αναθεώρησης**	**Αλλαγές**	**Ελέγχθηκε από**	**Ιδιοκτήτης διεργασίας**

Εγκρίσεις			
Όνομα	**Θέση**	**Ημερομηνία**	**Υπογραφή**

Ευθυγραμμισμένη με πρότυπα και κανονιστικές απαιτήσεις

Πρότυπο / Κανονιστική απαίτηση	Ρήτρα / Έλεγχος / Άρθρο	Εφαρμοσιμότητα	Τύπος κάλυψης	Σχόλιο
ISO/IEC 27701:2025	Clause 4.1	Both	Primary	Πλαίσιο ρόλου PIMS
ISO/IEC 27701:2025	Clause 5.1	Both	Primary	Ηγεσία και λογοδοσία
ISO/IEC 27701:2025	Clause 5.3	Both	Primary	Ρόλοι, αρμοδιότητες και εξουσίες PIMS
ISO/IEC 27701:2025	Clause 7.2	Both	Primary	Επάρκεια ρόλου
ISO/IEC 27701:2025	Clause 7.3	Both	Primary	Ευαισθητοποίηση ως προς τον ρόλο
ISO/IEC 27701:2025	Clause 7.4	Both	Supporting	Επικοινωνία ρόλου
ISO/IEC 27701:2025	Clause 7.5	Both	Primary	Τεκμηριωμένες πληροφορίες ρόλου
ISO/IEC 27701:2025	Clause 8.1	Both	Primary	Ιδιοκτησία επιχειρησιακών ελέγχων
ISO/IEC 27701:2025	Clause 9.2	Both	Supporting	Ανεξάρτητος ελεγκτικός ρόλος
ISO/IEC 27701:2025	Clause 9.3	Both	Supporting	Ανασκόπηση της λογοδοσίας από τη διοίκηση
ISO/IEC 27701:2025	Clause 10.2	Both	Supporting	Μη συμμόρφωση και διορθωτικά μέτρα σχετικά με ρόλους
ISO/IEC 27701:2025	Annex A.1.2.7	Controller	Supporting	Αρμοδιότητα σύμβασης εκτελούντος την επεξεργασία
ISO/IEC 27701:2025	Annex A.1.2.8	Joint Controller	Primary	Ρόλοι και αρμοδιότητες από κοινού υπευθύνων επεξεργασίας
ISO/IEC 27701:2025	Annex A.1.2.9	Controller	Primary	Αρχεία λογοδοσίας
ISO/IEC 27701:2025	Annex A.2.2.2	Processor	Primary	Συμφωνίες και εντολές πελατών

				για εκτελούντες την επεξεργασία
ISO/IEC 27701:2025	Annex A.2.2.3	Processor	Supporting	Ευθυγράμμιση σκοπού εκτελούντος την επεξεργασία
GDPR	Article 5(2)	Controller	Supporting	Τεκμήρια λογοδοσίας
GDPR	Article 24	Controller	Supporting	Ευθύνη και μέτρα υπευθύνου επεξεργασίας
GDPR	Article 26	Joint Controller	Supporting	Ρυθμίσεις από κοινού υπευθύνων επεξεργασίας
GDPR	Article 28	Both	Supporting	Διακυβέρνηση και εντολές εκτελούντος την επεξεργασία
GDPR	Article 30	Both	Supporting	Αρχεία επεξεργασίας και τεκμήρια αρμοδιότητας
GDPR	Article 37	Conditional	Referenced	Ορισμός DPO όπου εφαρμόζεται
GDPR	Article 38	Conditional	Supporting	Θέση και ανεξαρτησία DPO όπου εφαρμόζεται
GDPR	Article 39	Conditional	Supporting	Καθήκοντα DPO όπου εφαρμόζεται
ISO/IEC 29100:2020	Clause 4.1; Clause 4.2	Both	Supporting	Φορείς και ρόλοι πλαισίου ιδιωτικότητας
ISO/IEC 29100:2020	Clause 5.12	Both	Supporting	Λογοδοσία συμμόρφωσης ως προς την ιδιωτικότητα
ISO/IEC 29151:2022	Clause 6.1.2; Clause 6.1.3	Both	Supporting	Ρόλοι προστασίας PII και διαχωρισμός καθηκόντων
ISO/IEC 27002:2022	Control 5.2	Both	Supporting	Ρόλοι και αρμοδιότητες ασφάλειας πληροφοριών
ISO/IEC 27002:2022	Control 5.3	Both	Supporting	Διαχωρισμός καθηκόντων

1. Πεδίο εφαρμογής

1.1 Η παρούσα πολιτική καθορίζει το μοντέλο ρόλων PIMS, τη δομή λογοδοσίας, τους κανόνες ανάθεσης αρμοδιοτήτων, τους κανόνες συνδυασμού ρόλων, τις προσδοκίες κλιμάκωσης και τις απαιτήσεις τεκμηρίων για τη διακυβέρνηση ιδιωτικότητας.

1.2 Η παρούσα πολιτική εφαρμόζεται σε προσωπικό, λειτουργίες, συστήματα, προμηθευτές, εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας και σχέσεις από κοινού υπευθύνων επεξεργασίας που συμμετέχουν στην επεξεργασία PII ή την επηρεάζουν εντός του πεδίου εφαρμογής του PIMS.

1.3 Η παρούσα πολιτική εφαρμόζεται σε πλαίσια υπευθύνου επεξεργασίας, από κοινού υπευθύνου επεξεργασίας, εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας.

1.4 Η παρούσα πολιτική δεν δημιουργεί νέους οργανωτικούς τίτλους θέσεων. Καθορίζει τυποποιημένους ρόλους PIMS που μπορούν να ανατίθενται σε υφιστάμενο προσωπικό ή λειτουργίες, υπό την προϋπόθεση ότι τεκμηριώνονται οι απαιτήσεις ανάθεσης ρόλου, επάρκειας, ανεξαρτησίας και σύγκρουσης συμφερόντων.

2. Σκοπός

2.1 Σκοπός της παρούσας πολιτικής είναι να διασφαλίζει ότι οι αρμοδιότητες PIMS ανατίθενται με σαφήνεια, κατανοούνται, κοινοποιούνται, τεκμηριώνονται, ανασκοπούνται και βελτιώνονται.

2.2 Η παρούσα πολιτική επιτρέπει στον οργανισμό να αποδεικνύει λογοδοσία για τη διακυβέρνηση ιδιωτικότητας, την ιδιοκτησία επεξεργασίας PII, τον προσδιορισμό ρόλων υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία, την κατανομή ευθυνών από κοινού υπευθύνων επεξεργασίας, τον χειρισμό εντολών προς εκτελούντες την επεξεργασία, την αρμοδιότητα ιδιωτικότητας προμηθευτών, την ανεξάρτητη ανασκόπηση και την κλιμάκωση βάσει ρόλων.

3. Στόχοι

3.1 Οι στόχοι της παρούσας πολιτικής είναι:

3.1.1 να καθορίζει τους τυποποιημένους ρόλους PIMS που χρησιμοποιούνται στο σύνολο των πολιτικών PIMS·

3.1.2 να διασφαλίζει ότι κάθε ουσιώδης αρμοδιότητα PIMS έχει ανατεθειμένο υπόλογο ρόλο·

3.1.3 να υποστηρίζει τη λογοδοσία υπευθύνου επεξεργασίας, από κοινού υπευθύνου επεξεργασίας, εκτελούντος την επεξεργασία και υπεργολάβου επεξεργασίας·

3.1.4 να επιτρέπει τον πρακτικό συνδυασμό ρόλων για μικρούς και μεσαίους οργανισμούς, ελέγχοντας παράλληλα τις συγκρούσεις συμφερόντων·

3.1.5 να διατηρεί την ανεξάρτητη ανασκόπηση από Internal Audit / Compliance Reviewer·

3.1.6 να διασφαλίζει ότι οι αναθέσεις ρόλων και οι αλλαγές ρόλων καταγράφονται σε τυποποιημένα αντικείμενα τεκμηρίων·

3.1.7 να διασφαλίζει ότι οι κάτοχοι ρόλων PIMS λαμβάνουν κατάλληλη επικοινωνία και ευαισθητοποίηση·

3.1.8 να διασφαλίζει ότι κενά, συγκρούσεις και μη συμμορφώσεις σχετικά με ρόλους κλιμακώνονται και διορθώνονται.

4. Δηλώσεις πολιτικής

4.1 Μοντέλο και ανάθεση ρόλων PIMS

4.1.1 [All] Top Management πρέπει να εγκρίνει το τυποποιημένο μοντέλο ρόλων PIMS στο REG01 πριν από την αρχική υλοποίηση PIMS και ετησίως στη συνέχεια.

4.1.2 [All] Privacy Lead / PIMS Manager πρέπει να τηρεί ονομαστικές αναθέσεις ρόλων PIMS στο REG01 πριν από την υλοποίηση PIMS και εντός 10 εργάσιμων ημερών από αλλαγές προσωπικού ή οργανωτικές αλλαγές.

4.1.3 [All] Privacy Lead / PIMS Manager πρέπει να τεκμηριώνει το πεδίο αρμοδιοτήτων και το επίπεδο εξουσίας για κάθε ανατεθειμένο ρόλο PIMS στο REG01 πριν τεθεί σε ισχύ η ανάθεση.

4.1.4 [All] Process Owner / Business Owner πρέπει να αναθέτει υπόλογο ιδιοκτήτη επεξεργασίας για κάθε δραστηριότητα επεξεργασίας PII στο REG02 πριν από την έναρξη της δραστηριότητας επεξεργασίας.

4.1.5 [All] System Owner / Application Owner πρέπει να τεκμηριώνει τον υπόλογο ιδιοκτήτη συστήματος για κάθε σύστημα επεξεργασίας PII στο REG02 πριν από τη θέση του συστήματος σε λειτουργία.

4.1.6 [All] Vendor / Procurement Owner πρέπει να τεκμηριώνει τον ιδιοκτήτη σχέσης για κάθε σχέση εκτελούντος την επεξεργασία, υπεργολάβου επεξεργασίας, κοινοποίησης δεδομένων σε τρίτο μέρος ή από κοινού υπευθύνου επεξεργασίας στο REG08 πριν από την ένταξη ή την έγκριση συμφωνίας.

4.2 Συνδυασμός ρόλων, διαχωρισμός και ανεξαρτησία

4.2.1 [All] Privacy Lead / PIMS Manager πρέπει να τεκμηριώνει κάθε συνδυασμό ρόλων PIMS στο REG01 πριν τεθεί σε ισχύ ο συνδυασμός ρόλων.

4.2.2 [All] Top Management πρέπει να εγκρίνει στο REG01, πριν από την ανάθεση, συνδυασμούς ρόλων που αφορούν Privacy Lead / PIMS Manager, Data Protection Officer / Privacy Advisor, Information Security Lead, Incident Response Coordinator ή Internal Audit / Compliance Reviewer.

4.2.3 [All] Internal Audit / Compliance Reviewer πρέπει να τεκμηριώνει την ανεξαρτησία από τη διεργασία PIMS που ανασκοπείται στο REG12 πριν από την έναρξη κάθε ελέγχου PIMS ή ανασκόπησης συμμόρφωσης.

4.2.4 [All] Privacy Lead / PIMS Manager πρέπει να καταγράφει αντισταθμιστικούς ελέγχους για αναπόφευκτες συγκρούσεις διαχωρισμού καθηκόντων στο REG12 πριν εγκρίνει συνδυασμό ρόλων.

4.2.5 [All] Data Protection Officer / Privacy Advisor πρέπει να καταγράφει ζητήματα ανεξαρτησίας ρόλου ή ζητήματα σύγκρουσης συμφερόντων στο REG12 εντός πέντε εργάσιμων ημερών από την αναγνώρισή τους.

[... Οι ενότητες 4.3–8 δεν περιλαμβάνονται σε αυτή την προεπισκόπηση. Αγοράστε το πλήρες έγγραφο για πρόσβαση στο πλήρες περιεχόμενο. ...]

9. Εξαιρέσεις

9.1.1 [All] Process Owner / Business Owner πρέπει να ζητά εξαίρεση λογοδοσίας ρόλου στο REG12 πριν από τη λειτουργία δραστηριότητας επεξεργασίας PII χωρίς απαιτούμενο ανατεθειμένο ρόλο.

9.1.2 [All] Privacy Lead / PIMS Manager πρέπει να αξιολογεί τον αντίκτυπο και τον μετριασμό κάθε εξαίρεσης λογοδοσίας ρόλου στο REG12 εντός 10 εργάσιμων ημερών από το αίτημα.

9.1.3 [All] Top Management πρέπει να εγκρίνει εξαιρέσεις λογοδοσίας ρόλου που υπερβαίνουν τις 30 ημέρες ή επηρεάζουν επεξεργασία υψηλού κινδύνου στο REG12 πριν τεθεί σε ισχύ η εξαίρεση.

9.1.4 [All] Privacy Lead / PIMS Manager πρέπει να ορίζει ημερομηνία λήξης που δεν υπερβαίνει τις 90 ημέρες στο REG12 για κάθε εγκεκριμένη εξαίρεση λογοδοσίας ρόλου πριν από την έγκριση.

9.1.5 [All] Privacy Lead / PIMS Manager πρέπει να κλείνει ή να επαναξιολογεί κάθε εξαίρεση λογοδοσίας ρόλου στο REG12 εντός πέντε εργάσιμων ημερών από τη λήξη.

10. Εφαρμογή

10.1.1 [All] Privacy Lead / PIMS Manager πρέπει να καταγράφει ελλείπουσες, ανακριβείς ή παρωχημένες αναθέσεις ρόλων PIMS ως μη συμμορφώσεις στο REG12 εντός πέντε εργάσιμων ημερών από την αναγνώρισή τους.

10.1.2 [All] Top Management πρέπει να απαιτεί διορθωτικά μέτρα στο REG12 εντός 15 εργάσιμων ημερών για επαναλαμβανόμενες ή παρατεταμένες αστοχίες λογοδοσίας.

10.1.3 [All] Process Owner / Business Owner πρέπει να αποτρέπει τη θέση σε λειτουργία νέας ή τροποποιημένης επεξεργασίας PII όταν τα απαιτούμενα τεκμήρια ρόλου και λογοδοσίας απουσιάζουν από το REG02 ή το REG08.

10.1.4 [All] Internal Audit / Compliance Reviewer πρέπει να επαληθεύει την αποτελεσματικότητα διορθωτικών μέτρων για μη συμμορφώσεις λογοδοσίας ρόλου στο REG12 κατά τον επόμενο προγραμματισμένο έλεγχο ή εντός 60 ημερών από το κλείσιμο, όποιο επέλθει πρώτο.

11. Ανασκόπηση και συντήρηση

11.1.1 [All] Privacy Lead / PIMS Manager πρέπει να ανασκοπεί την παρούσα πολιτική ετησίως και εντός 30 ημερών από ουσιώδη αλλαγή στο μοντέλο ρόλων PIMS.

11.1.2 [All] Data Protection Officer / Privacy Advisor πρέπει να ανασκοπεί προτεινόμενες αλλαγές στην παρούσα πολιτική ως προς τον αντίκτυπο στους ρόλους ιδιωτικότητας στο REG12 πριν από την έγκριση.

11.1.3 [All] Top Management πρέπει να εγκρίνει ουσιώδεις αλλαγές στην παρούσα πολιτική στο REG12 πριν από τη δημοσίευση.

11.1.4 [All] Privacy Lead / PIMS Manager πρέπει να επικαιροποιεί το REG01 και το REG11 εντός 15 εργάσιμων ημερών μετά από εγκεκριμένες αλλαγές σε ρόλους, αρμοδιότητες ή απαιτήσεις επικοινωνίας PIMS.

12. Συναφείς πολιτικές

12.1 Η παρούσα πολιτική υποστηρίζεται από τις ακόλουθες συναφείς πολιτικές:

12.1.1 PII01 - Πολιτική Συστήματος Διαχείρισης Πληροφοριών Ιδιωτικότητας

12.1.2 PII03 - Πολιτική απογραφής επεξεργασίας PII και νομικής βάσης

12.1.3 PII07 - Πολιτική αξιολόγησης κινδύνου ιδιωτικότητας και DPIA

12.1.4 PII08 - Πολιτική προστασίας της ιδιωτικότητας ήδη από τον σχεδιασμό και εξ ορισμού

12.1.5 PII12 - Πολιτική διαχείρισης ιδιωτικότητας εκτελούντων την επεξεργασία, υπεργολάβων επεξεργασίας και τρίτων μερών

12.1.6 PII14 - Πολιτική ασφάλειας PII και ελέγχου πρόσβασης

12.1.7 PII15 - Πολιτική διαχείρισης περιστατικών και παραβιάσεων PII

12.1.8 PII16 - Πολιτική εκπαίδευσης, ευαισθητοποίησης και επάρκειας ιδιωτικότητας

12.1.9 PII17 - Πολιτική τεκμηριωμένων πληροφοριών και διαχείρισης τεκμηρίων PIMS

12.1.10 PII18 - Πολιτική παρακολούθησης, ελέγχου και βελτίωσης PIMS

13. Πρότυπα και πλαίσια αναφοράς

13.1 Η παρούσα πολιτική αντιστοιχίζεται στα ακόλουθα πρότυπα και κανονιστικές απαιτήσεις. Η αντιστοίχιση εξηγεί πώς η πολιτική υποστηρίζει τις αναφερόμενες απαιτήσεις και προσδιορίζει τις εσωτερικές ρήτρες που τις υλοποιούν ή τις υποστηρίζουν.

13.2 ISO/IEC 27701:2025

13.2.1 **Clause 4.1** - Αντιστοιχίζεται στον προσδιορισμό του πλαισίου ρόλων PIMS, της εφαρμοσιμότητας υπευθύνου επεξεργασίας και εκτελούντος την επεξεργασία, της ιδιοκτησίας επεξεργασίας και των αρχείων αρμοδιότητας σχέσεων. Addressed by clauses [4.3.5; 5.1.5; 5.1.7; 7.1.2].

13.2.2 **Clause 5.1** - Αντιστοιχίζεται στην έγκριση από Top Management, την εποπτεία λογοδοσίας, την ετήσια ανασκόπηση της διοίκησης, τις μετρικές λογοδοσίας και τα διορθωτικά μέτρα για αστοχίες ρόλων. Addressed by clauses [4.1.1; 4.2.2; 5.1.1; 6.1.1; 8.1.6; 10.1.2; 11.1.3].

13.2.3 **Clause 5.3** - Αντιστοιχίζεται στην ανάθεση, τεκμηρίωση, κοινοποίηση και συντήρηση ρόλων, αρμοδιοτήτων και εξουσιών PIMS, στην ιδιοκτησία συστημάτων, την ιδιοκτησία επεξεργασίας, την ιδιοκτησία σχέσεων προμηθευτών, την ιδιοκτησία κλιμάκωσης περιστατικών και την αρμοδιότητα ανεξάρτητης ανασκόπησης. Addressed by clauses [4.1.2; 4.1.3; 4.1.4; 4.1.5; 4.1.6; 4.4.2; 4.4.3; 5.1.2; 5.1.3; 5.1.4; 5.1.5; 5.1.6; 5.1.7; 5.1.8; 5.1.9].

13.2.4 **Clause 7.2** - Αντιστοιχίζεται σε τεκμήρια επάρκειας και ευαισθητοποίησης ειδικά ανά ρόλο για τις ανατεθειμένες αρμοδιότητες PIMS. Addressed by clauses [7.1.4; 8.1.5].

13.2.5 **Clause 7.3** - Αντιστοιχίζεται στην ευαισθητοποίηση ως προς τις ανατεθειμένες αρμοδιότητες PIMS, στα τεκμήρια αναγνώρισης και στην ετήσια αναφορά ευαισθητοποίησης ρόλων. Addressed by clauses [4.5.1; 4.5.2; 7.1.4; 8.1.5].

13.2.6 **Clause 7.4** - Αντιστοιχίζεται στην επικοινωνία αναθέσεων ρόλων, αλλαγών ρόλων, κλιμακώσεων και πληροφοριών παράδοσης ρόλων. Addressed by clauses [4.5.1; 4.5.4; 6.1.5; 7.1.6].

13.2.7 **Clause 7.5** - Αντιστοιχίζεται σε τεκμηριωμένες πληροφορίες για αναθέσεις ρόλων PIMS, πεδία αρμοδιοτήτων, επίπεδα εξουσίας, ετήσια διατήρηση τεκμηρίων και συντήρηση της μήτρας ρόλων. Addressed by clauses [4.1.2; 4.1.3; 4.5.3; 7.1.1; 11.1.4].

13.2.8 **Clause 8.1** - Αντιστοιχίζεται στην ιδιοκτησία επιχειρησιακών ελέγχων για δραστηριότητες επεξεργασίας, συστήματα, προμηθευτές, εκτελούντες την επεξεργασία, υπεργολάβους επεξεργασίας, σχέσεις από κοινού υπευθύνων επεξεργασίας και ελέγχους θέσης σε λειτουργία. Addressed by clauses [4.1.4; 4.1.5; 4.1.6; 7.1.2; 7.1.3; 7.1.5; 10.1.3].

13.2.9 **Clause 9.2** - Αντιστοιχίζεται στον ανεξάρτητο έλεγχο και την ανασκόπηση συμμόρφωσης των τεκμηρίων ανάθεσης ρόλων, τεκμηρίων συνδυασμού ρόλων, τεκμηρίων ανεξαρτησίας, ευρημάτων και κλεισίματος διορθωτικών ενεργειών. Addressed by clauses [4.2.3; 5.1.9; 6.1.4; 8.1.4; 10.1.4].

13.2.10 **Clause 9.3** - Αντιστοιχίζεται στην ανασκόπηση από τη διοίκηση της πληρότητας αναθέσεων ρόλων PIMS, των συγκρούσεων ρόλων, των εξαιρέσεων, των μετρικών λογοδοσίας και των αποτελεσμάτων ανασκόπησης λογοδοσίας. Addressed by clauses [5.1.1; 6.1.1; 8.1.6; 11.1.1].

13.2.11 **Clause 10.2** - Αντιστοιχίζεται στην κλιμάκωση, την καταγραφή μη συμμόρφωσης, τα διορθωτικά μέτρα, το κλείσιμο εξαιρέσεων και την επαλήθευση αποτελεσματικότητας για ζητήματα λογοδοσίας ρόλων. Addressed by clauses [4.2.5; 4.4.5; 6.1.5; 9.1.5; 10.1.1; 10.1.2; 10.1.4].

13.2.12 **Annex A.1.2.7** - Αντιστοιχίζεται στην ανάθεση και τεκμηρίωση αρμοδιότητας συμβάσεων εκτελούντων την επεξεργασία και κλιμάκωσης αρμοδιοτήτων τρίτων μερών πριν από την έγκριση ή ανανέωση σύμβασης. Addressed by clauses [4.1.6; 4.4.4; 5.1.7; 7.1.3].

13.2.13 **Annex A.1.2.8** - Αντιστοιχίζεται στην τεκμηρίωση της κατανομής ευθυνών από κοινού υπευθύνων επεξεργασίας και των τεκμηρίων αρμοδιότητας σχέσεων πριν από την έναρξη επεξεργασίας από κοινού υπευθύνων επεξεργασίας. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.2.14 **Annex A.1.2.9** - Αντιστοιχίζεται στην τήρηση αρχείων λογοδοσίας για την ιδιοκτησία επεξεργασίας από υπεύθυνο επεξεργασίας, την ταξινόμηση ρόλων και την ιδιοκτησία τεκμηρίων. Addressed by clauses [4.3.1; 4.3.5; 4.5.3; 8.1.1].

13.2.15 **Annex A.2.2.2** - Αντιστοιχίζεται στην αρμοδιότητα συμφωνίας πελάτη για εκτελούντα την επεξεργασία, τον υπεύθυνο εντολών πελάτη και τα τεκμήρια σχέσης εκτελούντος την επεξεργασία. Addressed by clauses [4.3.3; 5.1.7; 7.1.3; 8.1.3].

13.2.16 **Annex A.2.2.3** - Αντιστοιχίζεται στην ευθυγράμμιση σκοπού και εντολών εκτελούντος την επεξεργασία μέσω υπευθύνου εντολών πελάτη και επαλήθευσης ρόλων υπευθύνου επεξεργασίας/εκτελούντος την επεξεργασία. Addressed by clauses [4.3.3; 4.3.5; 5.1.7].

13.3 GDPR

13.3.1 **Article 5(2)** - Αντιστοιχίζεται σε τεκμήρια λογοδοσίας για αναθέσεις ρόλων, ιδιοκτησία επεξεργασίας, ανασκοπήσεις ρόλων, μη συμμορφώσεις και ευρήματα ελέγχου. Addressed by clauses [4.5.3; 6.1.2; 8.1.1; 10.1.1].

13.3.2 **Article 24** - Αντιστοιχίζεται στην ευθύνη υπευθύνου επεξεργασίας, την υπόλογη ιδιοκτησία επεξεργασίας, την εποπτεία από Top Management, την ετήσια ανασκόπηση και τα μέτρα λογοδοσίας. Addressed by clauses [4.1.1; 4.3.1; 5.1.1; 6.1.1; 8.1.6].

13.3.3 **Article 26** - Αντιστοιχίζεται στην τεκμηρίωση της κατανομής ευθυνών από κοινού υπευθύνων επεξεργασίας και των τεκμηρίων αρμοδιότητας σχέσεων πριν από την έναρξη επεξεργασίας από κοινού υπευθύνων επεξεργασίας. Addressed by clauses [4.3.2; 5.1.7; 7.1.3; 8.1.3].

13.3.4 **Article 28** - Αντιστοιχίζεται στην κατανομή ευθυνών εκτελούντων την επεξεργασία και υπεργολάβων επεξεργασίας, τον υπεύθυνο εντολών πελάτη, την αρμοδιότητα σύμβασης και τις διαδρομές κλιμάκωσης τρίτων μερών. Addressed by clauses [4.3.3; 4.3.4; 4.4.4; 5.1.7; 7.1.3].

13.3.5 **Article 30** - Αντιστοιχίζεται στα αρχεία επεξεργασίας, την ιδιοκτησία επεξεργασίας, την ταξινόμηση ρόλων PIMS και την επαλήθευση ρόλων υπευθύνου επεξεργασίας/εκτελούντος την επεξεργασία. Addressed by clauses [4.1.4; 4.3.1; 4.3.5; 8.1.1].

13.3.6 **Article 37** - Αντιστοιχίζεται στην τεκμηρίωση του ρόλου Data Protection Officer / Privacy Advisor όπου ο ορισμός εφαρμόζεται ή γίνεται οικειοθελώς. Addressed by clauses [4.1.2; 4.1.3; 5.1.3; 11.1.2].

13.3.7 **Article 38** - Αντιστοιχίζεται στη θέση, την ανεξαρτησία, τη συμμετοχή και τον χειρισμό σύγκρουσης συμφερόντων του Data Protection Officer / Privacy Advisor όπου εφαρμόζεται. Addressed by clauses [4.2.5; 5.1.3; 6.1.3; 11.1.2].

13.3.8 **Article 39** - Αντιστοιχίζεται στις συμβουλές ιδιωτικότητας, τις παρατηρήσεις παρακολούθησης, τη συμβουλευτική ανασκόπηση και την ανασκόπηση αντικτύπου στους ρόλους ιδιωτικότητας από Data Protection Officer / Privacy Advisor όπου εφαρμόζεται. Addressed by clauses [4.4.1; 5.1.3; 6.1.3; 11.1.2].

13.4 ISO/IEC 29100:2020

13.4.1 **Clause 4.1; Clause 4.2** - Αντιστοιχίζεται σε φορείς πλαισίου ιδιωτικότητας και κατανομή ρόλων για υποκείμενα των δεδομένων προσωπικού χαρακτήρα, υπευθύνους επεξεργασίας PII, εκτελούντες την επεξεργασία PII, τρίτα μέρη και ταξινόμηση ρόλων PIMS. Addressed by clauses [4.1.4; 4.1.6; 4.3.5; 5.1.5; 5.1.7].

13.4.2 **Clause 5.12** - Αντιστοιχίζεται στη λογοδοσία συμμόρφωσης ως προς την ιδιωτικότητα, τα τεκμήρια ρόλων, την ανασκόπηση, τα ευρήματα ελέγχου και την επαλήθευση διορθωτικών ενεργειών. Addressed by clauses [4.5.3; 6.1.2; 8.1.4; 10.1.4].

13.5 ISO/IEC 29151:2022

13.5.1 **Clause 6.1.2; Clause 6.1.3** - Αντιστοιχίζεται στον ορισμό ρόλων προστασίας PII, την τεκμηρίωση ρόλων, την επικοινωνία ρόλων, τον συντονισμό ασφάλειας/ιδιωτικότητας και τον

διαχωρισμό καθηκόντων για την προστασία PII. Addressed by clauses [4.1.1; 4.2.1; 4.2.3; 4.2.4; 4.4.2; 5.1.4; 7.1.4].

13.6 ISO/IEC 27002:2022

13.6.1 Control 5.2 - Αντιστοιχίζεται στον καθορισμό, την κατανομή, την τεκμηρίωση, την κοινοποίηση και τη συντήρηση αρμοδιοτήτων PIMS και ασφάλειας πληροφοριών. Addressed by clauses [4.1.1; 4.1.2; 4.1.3; 4.2.1; 4.4.2; 4.5.1; 5.1.4; 7.1.1].

13.6.2 Control 5.3 - Αντιστοιχίζεται στον διαχωρισμό καθηκόντων, την έγκριση συνδυασμού ρόλων, την ανεξάρτητη ανασκόπηση, τους ελέγχους συγκρούσεων και την επαλήθευση διορθωτικών ενεργειών για συγκρούσεις ρόλων. Addressed by clauses [4.2.2; 4.2.3; 4.2.4; 9.1.2; 10.1.4].