ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΝΟΜΟΣ ΚΥΚΛΑΔΩΝ

Μύκονος, 30 Δεκεμβρίου 2025
Αριθμ. Πρωτ. 32147

ΔΗΜΟΣ ΜΥΚΟΝΟΥ

Πληροφορίες: Τουλουμτζή Παναγιώτα
Τηλέφωνο : 2289360147
email: p.touloumtzi@mykonos.gr

ΣΥΜΦΩΝΗΤΙΚΟ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΑΣ

«Ετήσια Παροχή Ανεξάρτητων Υπηρεσιών Υποστήριξης της Υπηρεσίας Εσωτερικού Ελέγχου»

(συνολικού ποσού 37.200,00 € συμπεριλαμβανομένου Φ.Π.Α.)

Στη Μύκονο σήμερα στις 30 του μηνός Δεκεμβρίου του έτους 2025, ημέρα της εβδομάδας Τρίτη μεταξύ:

- Του Δήμου Μυκόνου με ΑΦΜ:090235079 ο οποίος νόμιμα εκπροσωπείται από τον κ.Βερώνη Χρήστο, Δήμαρχο Μυκόνου, σύμφωνα με τις διατάξεις του άρθρου 58 του Ν.3852/10 «Νέα Αρχιτεκτονική της Αυτοδιοίκησης και της Αποκεντρωμένης Διοίκησης – Πρόγραμμα Καλλικράτης», που για λόγους συντομίας στο παρόν συμφωνητικό θα αναφέρεται ως ‘‘εργοδότης” και
- Του οικονομικού φορέα «PUBLIC AUDIT SERVICES ΕΕ» με έδρα τον Πειραιά, οδός Ν.Νοταρά 45 Τ.Κ.18531 Α.Φ.Μ.: 802035894, Δ.Ο.Υ.:Α Πειραιά Email:info@publicauditservices.gr που εκπροσωπείται νόμιμα από την κ.Άννα Συρρή, που για λόγους συντομίας στο παρόν συμφωνητικό θα αναφέρεται ως ‘‘ανάδοχος’’,

και έχοντας υπόψη:

1. τις διατάξεις του Ν.4412/16 «Δημόσιες Συμβάσεις Έργων, Προμηθειών και Υπηρεσιών (προσαρμογή στις Οδηγίες 2014/24/ΕΕ και 2014/25/ΕΕ)»,
2. τις διατάξεις του Ν.3463/06 «Κύρωση του Κώδικα Δήμων και Κοινοτήτων» και ιδίως του άρθρου 209,
3. τις διατάξεις του Ν.3852/10 «Νέα Αρχιτεκτονική της Αυτοδιοίκησης και της Αποκεντρωμένης Διοίκησης – Πρόγραμμα Καλλικράτης»,
4. τις διατάξεις του Ν.4555/18 «Μεταρρύθμιση του θεσμικού πλαισίου της Τοπικής Αυτοδιοίκησης - Εμβάθυνση της Δημοκρατίας - Ενίσχυση της Συμμετοχής - Βελτίωση της οικονομικής και αναπτυξιακής λειτουργίας των Ο.Τ.Α. [Πρόγραμμα «ΚΛΕΙΣΘΕΝΗΣ Ι»] -Ρυθμίσεις για τον εκσυγχρονισμό του πλαισίου οργάνωσης και λειτουργίας των ΦΟΔΣΑ

- Ρυθμίσεις για την αποτελεσματικότερη, ταχύτερη και ενιαία άσκηση των αρμοδιοτήτων σχετικά με την απονομή ιθαγένειας και την πολιτογράφηση - Λοιπές διατάξεις αρμοδιότητας Υπουργείου Εσωτερικών και άλλες διατάξεις.»,

5. τις διατάξεις του Ν.4270/14 «Αρχές δημοσιονομικής διαχείρισης και εποπτείας (ενσωμάτωση της Οδηγίας 2011/85/ΕΕ) – δημόσιο λογιστικό και άλλες διατάξεις»,
6. τις διατάξεις της Κ.Υ.Α. 76928/21 «Ρύθμιση ειδικότερων θεμάτων λειτουργίας και διαχείρισης του Κεντρικού Ηλεκτρονικού Μητρώου Δημοσίων Συμβάσεων (ΚΗΜΔΗΣ)»,
7. τις διατάξεις του Π.Δ. 80/16 «Ανάληψη υποχρεώσεων από τους Διατάκτες»,
8. τις διατάξεις της παραγράφου Ζ' του άρθρου 1 του Ν.4152/13
9. «Επείγοντα μέτρα εφαρμογής των νόμων 4046/2012, 4093/2012 και 4127/2013»,
10. τα άρθρα 148-154 του ν. 4601/2019 (Α' 44) «Εταιρικοί μετασχηματισμοί και εναρμόνιση του νομοθετικού πλαισίου με τις διατάξεις της Οδηγίας 2014/55/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 16ης Απριλίου 2014 για την έκδοση ηλεκτρονικών τιμολογίων στο πλαίσιο δημόσιων συμβάσεων και λοιπές διατάξεις», ως ισχύουν
11. της Κ.Υ.Α. 52445 ΕΞ 2023 (Β' 2385/12.04.2023) «Υποχρέωση υποβολής ηλεκτρονικών τιμολογίων από τους οικονομικούς φορείς» ως ισχύει
12. της Κ.Υ.Α. 63446/2021 (Β' 2338/02.06.2021) «Καθορισμός Εθνικού Μορφότυπου ηλεκτρονικού τιμολογίου στο πλαίσιο των Δημοσίων Συμβάσεων» ως ισχύει
13. της Κ.Υ.Α. οικ. 98979 ΕΞ2021 (Β' 3766/13.08.2021) «Ηλεκτρονική
14. Τιμολόγηση στο πλαίσιο των Δημόσιων Συμβάσεων δυνάμει του ν. 4601/2019» ως ισχύει
15. Την ανάγκη του Δήμου για την πραγματοποίηση της συγκεκριμένης δαπάνης.
16. Την ανάγκη του Δήμου για την πραγματοποίηση της συγκεκριμένης δαπάνης.
17. Την υπ.αριθ.716 /2025 απόφαση αναγκαιότητας με ΑΔΑ:68Χ4ΩΚΚ-ΚΒ4.
18. Την υπ.αριθ.09/2025 μελέτη με τίτλο "Ετήσια Παροχή Ανεξάρτητων Υπηρεσιών Υποστήριξης της Υπηρεσίας Εσωτερικού Ελέγχου" που συνέταξε η Δ/νση Διοικητικών του Δήμου.
19. Το υπ' αριθ. 31234/15-12-2025 πρωτογενές αίτημα για την "Ετήσια Παροχή Ανεξάρτητων Υπηρεσιών Υποστήριξης της Υπηρεσίας Εσωτερικού Ελέγχου" που συνέταξε η Δ/νση Διοικητικών και αναρτήθηκε στο ΚΗΜΔΗΣ με ΑΔΑΜ:25REQ018171677/15-12-2025.
20. Τον προϋπολογισμό του Δήμου οικ. έτους 2025 και συγκεκριμένα τις εγγεγραμμένες πιστώσεις στον υπό Κ.Α. 10-6142.0021.

21. Την υπ.αριθ.771/2025 Απόφαση έγκρισης πολυετούς υποχρέωσης με ΑΔΑ: ΡΝΞ0ΩΚΚ-4ΙΔ συνολικού ποσού 37.200,00 € για το έτος 2026 σε βάρος του ΚΑΕ.10-6142.0021 και ΑΔΑΜ:25REQ018207913/18-12-2025.
22. Την υπ.αριθ.774/2025 απόφαση Δημάρχου με ΑΔΑ: ΛΨΘΖΩΚΚ-ΟΕΑ.
23. Την με αριθ.πρωτ.31553/18-12-2025 πρόσκληση υποβολής προσφοράς με ΑΔΑΜ:25PROC018208646/18-12-2025.
24. Την υπ.αριθ.31923/24-12-2025 υποβληθείσα προσφορά του οικονομικού φορέα PUBLIC AUDIT SERVICES ΕΕ ύψους 30.000,00€ πλέον ΦΠΑ 24% ποσού 7.200,00€ συνολικού κόστους 37.200,00€ η οποία κρίνεται η πλέον συμφέρουσα για τον Δήμο από οικονομική άποψη βάσει της τιμής, διότι καλύπτει τις απαιτήσεις της υπηρεσίας.
25. Το γεγονός ότι η προσφορά και τα δικαιολογητικά υπεβλήθησαν προσηκόντως και η προσφορά περιελάμβανε τα απαιτούμενα αποδεικτικά μέσα και δικαιολογητικά.
26. την υπ' αριθ. 822/2025 απόφαση ανάθεσης του Δημάρχου η οποία καταχωρήθηκε στο ΚΗΜΔΗΣ λαμβάνοντας ΑΔΑΜ: 25AWRD018276587 και στο πρόγραμμα «ΔΙΑΥΓΕΙΑ» λαμβάνοντας ΑΔΑ:6Δ2ΩΩΚΚ-3ΨΣ και κοινοποιήθηκε στον οικονομικό φορέα με μήνυμα ηλεκτρονικού ταχυδρομείου στις 30-12-2025.
27. την ανάγκη του Δήμου για την υλοποίηση της παροχής υπηρεσίας.

Συμφωνήθηκαν, συνομολογήθηκαν και έγιναν αμοιβαίως αποδεκτά τα ακόλουθα:

ΑΡΘΡΟ 1ο: Αντικείμενο σύμβασης – Συμβατικό ποσό

Αντικείμενο του παρόντος συμφωνητικού αποτελεί η εκτέλεση της παροχής υπηρεσίας "Ετήσια Παροχή Ανεξάρτητων Υπηρεσιών Υποστήριξης της Υπηρεσίας Εσωτερικού Ελέγχου" ύψους 30.000,00 € πλέον Φ.Π.Α. 24%, ποσού 7.200,00€, ήτοι σύνολο 37.200,00€ με βάση την υποβληθείσα προσφορά του αναδόχου, η οποία έχει ως εξής:

ΠΕΡΙΓΡΑΦΗ	**Μον. Μέτρ.**	**ΠΟΣΟΤΗΤΑ**	**ΔΑΠΑΝΗ**
Παροχή ανεξάρτητων υπηρεσιών υποστήριξης της λειτουργίας Εσωτερικού Ελέγχου του Δήμου Μυκόνου	Παραδοτέο 1	1	2.000,00
	Παραδοτέο 2	1	5.500,00
	Παραδοτέο 3	1	5.500,00
	Παραδοτέο 4	1	5.500,00
	Παραδοτέο 5	1	8.000,00
	Παραδοτέο 6	1	3.500,00

Σύνολο καθαρής αξίας	30.000,00
ΦΠΑ 24%	7.200,00

Στο ανωτέρω ποσό ο ανάδοχος έχει συμπεριλάβει όλα τα έξοδα που μπορεί να απαιτηθούν για την ορθή και έγκαιρη εκτέλεση των ανωτέρω υπηρεσιών στον Δήμο, συμπεριλαμβανομένων και των τυχόν εξόδων ασφάλισης, αμοιβής, μετακίνησης, διαμονής και σίτισης του προσωπικού ή/και των συνεργατών που θα απασχολήσει κ.ά.

ΑΡΘΡΟ 2ο: Έγγραφα της σύμβασης

Τα έγγραφα της σύμβασης, κατά σειρά ισχύος, είναι:

- Το συμφωνητικό
- Η υπ' αριθ. 09/2025 μελέτη
- Η απόφαση ανάθεσης
- Η προσφορά του αναδόχου συμπεριλαμβανομένων των αποδεικτικών μέσων

ΑΡΘΡΟ 3ο: Ύπαρξη πίστωσης - Χρηματοδότηση

Για την πραγματοποίηση της παρούσας παροχής υπηρεσίας υπάρχει επαρκής, διαθέσιμη και εξειδικευμένη πίστωση στον προϋπολογισμό του Δήμου οικονομικού έτους 2025 & 2026 και συγκεκριμένα στον κωδικό ΚΑ.10-6142.0021.

Η παρούσα δαπάνη χρηματοδοτείται από ιδίους πόρους του Δήμου.

ΑΡΘΡΟ 4ο: Ισχύς σύμβασης

Το παρόν συμφωνητικό, το οποίο έχει αποδεικτικό χαρακτήρα, τίθεται σε ισχύ από την ημερομηνία υπογραφής και ανάρτησης του στο ΚΗΜΔΗΣ, ενώ ο χρόνος εκτέλεσης της παροχής υπηρεσίας ορίζεται για 12 μήνες.

ΑΡΘΡΟ 5ο: Παρακολούθηση και παραλαβή υπηρεσιών

Για την εκτέλεση της υπηρεσίας εφαρμόζονται οι διατάξεις του Ν. 4412/16 και ιδίως των άρθρων 200 – 205 και 216 – 220. Η παρακολούθηση της σύμβασης και η διοίκηση αυτής θα πραγματοποιηθεί από την Δ/νση Διοικητικών.

Η παραλαβή των υπηρεσιών θα πραγματοποιηθεί από την κατά νόμο αρμόδια επιτροπή παραλαβής υπηρεσιών.

ΑΡΘΡΟ 6ο: Σταθερότητα τιμών

Η τιμή μονάδας της προσφοράς θα είναι σταθερή και αμετάβλητη κατά τη διάρκεια εκτέλεσης της σύμβασης και για κανένα λόγο και σε καμία αναθεώρηση δεν υπόκειται.

Για την πληρωμή του αναδόχου απαραίτητη προϋπόθεση είναι η έκδοση ηλεκτρονικού τιμολογίου σύμφωνα με τα οριζόμενα στο ν.4601/2019

Η έκδοση ηλεκτρονικού τιμολογίου γίνεται αποκλειστικά μέσω των πιστοποιημένων παρόχων ηλ.τιμολόγησης που αναρτώνται στον παρακάτω ιστότοπο:

https://www.gsis.gr/polites-epiheiriseis/pliromes-kai-eispraxeis/e-invoice/parohoi-ypiresion-ilektronikis-timologisis

ΑΡΘΡΟ 7ο: Πληρωμή αναδόχου

Η πληρωμή θα γίνεται σταδιακά από την ταμειακή υπηρεσία του Δήμου, κατόπιν έκδοσης χρηματικού εντάλματος πληρωμής από την Οικονομική Υπηρεσία του Δήμου στο όνομα του αναδόχου, βάσει της αναληφθείσας υποχρέωσης σε βάρος του οικείου κωδικού αριθμού του προϋπολογισμού του Δήμου οικονομικού έτους 2025 & 2026, μετά την έκδοση των σχετικών τιμολογίων και την υπογραφή των σχετικών πρωτοκόλλων παραλαβής από την επιτροπή παραλαβής υπηρεσιών στο 100% της αξίας των εκτελεσθέντων υπηρεσιών.

Σύμφωνα με την παρ.2γ' του άρθρου 1 της Αριθμ.ΚΥΑ 52445 ΕΞ 2023/23 (ΦΕΚ 2385 Β/12-4-2023-Διορθ.σφαλμ. Στο ΦΕΚ 3061 Β/9-5-23) με θέμα : Υποχρέωση υποβολής ηλεκτρονικών τιμολογίων από τους οικονομικούς φορείς, οι οικονομικοί φορείς υποχρεούνται να υποβάλλουν ηλεκτρονικά τιμολόγια που είναι σύμφωνα με το ευρωπαϊκό πρότυπο έκδοσης ηλεκτρονικών τιμολογίων (PEPPOL) και τον εθνικό μορφότυπο κατά τα οριζόμενα στον ν.4601/2019 και στην ΚΥΑ 63446/2021 ως ισχύουν.

Επισημαίνεται ότι δεν συνιστούν ηλεκτρονικό τιμολόγιο, τα τιμολόγια των κάτωθι περιπτώσεων i ως iv, και ως εκ τούτου δεν υπάρχει δυνατότητα αποδοχής τους προς πληρωμή

i.Απλό αρχείο εικόνας (jpeg/png)

ii. Σκαναρισμένο έγχαρτο τιμολόγιο σε μορφή pdf ή άλλη μορφή που αποστέλλεται με ηλεκτρονικά μέσα.

iii. Τιμολόγιο που εκδίδεται μέσω της εφαρμογής "timologio" της ΑΑΔΕ η οποία παρέχει τη δυνατότητα στους οικονομικούς φορείς μηχανογραφικής έκδοσης και αυτόματης διαβίβασης τιμολογίων στην πλατφόρμα myData της ΑΑΔΕ.

iv. Τιμολόγιο που δεν έχει δρομολογηθεί στον Δήμο Μυκόνου μέσω του Κέντρου Διαλειτουργικότητας (ΚΕΔ)

ΑΡΘΡΟ 8ο: Χρονική παράταση σύμβασης

Τυχόν χρονική παράταση της εν λόγω διαδικασίας ορίζεται σύμφωνα με το άρθρο του 217 του Ν. 4412/16.

ΑΡΘΡΟ 9ο: Ζημιές – Ατυχήματα

Ο ανάδοχος έχει υποχρέωση και ευθύνη να λαμβάνει όλα τα αναγκαία μέτρα για την ασφάλεια του προσωπικού που απασχολεί κατά την εκτέλεση της σύμβασης και για την πρόληψη ζημιών – ατυχημάτων σε οποιαδήποτε πρόσωπα ή πράγματα. Για ατυχήματα ή ζημιές που τυχόν θα συμβούν στο προσωπικό του αναδόχου ή οποιονδήποτε τρίτο, ο Δήμος δεν έχει καμιά ευθύνη και ο ανάδοχος έχει αποκλειστικά τις ευθύνες, τόσο τις αστικές όσο και τις ποινικές, σύμφωνα με τις διατάξεις των οικείων νόμων για τις περιπτώσεις αυτές.

ΑΡΘΡΟ 10ο: Κρατήσεις

Ο ανάδοχος υπόκειται σε όλες τις νόμιμες κρατήσεις, πλην του Φ.Π.Α. ο οποίος βαρύνει τον εργοδότη.

ΑΡΘΡΟ 11ο: Επίλυση διαφορών

Τυχόν διαφορές μεταξύ του εργοδότη και του αναδόχου, επιλύονται σύμφωνα με τα οριζόμενα στους Ν.3463/06, Ν.3852/10 και Ν.4412/16 και συμπληρωματικά στον Αστικό Κώδικα, καθώς και τυχόν παράλληλης σχετικής νομοθεσίας που είναι σε ισχύ.

ΑΡΘΡΟ 12ο : Συμμόρφωση με τον Κανονισμό ΕΕ/2016/2019 και τον ν. 4624/2019 (Α 137)

Τα αντισυμβαλλόμενα μέρη αναλαμβάνουν να τηρούν τις υποχρεώσεις που απορρέουν από την εφαρμογή του Κανονισμού (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός Προστασίας Δεδομένων / General Data Protection Regulation – GDPR) και του Ν. 4624/2019.

Ειδικότερα:
Α) Ως προς την επεξεργασία από την Αναθέτουσα Αρχή των προσωπικών δεδομένων του Αναδόχου συμπεριλαμβανομένων των προστηθέντων/συνεργατών/δανειζόντων εμπειρία/υπεργολάβων του, ισχύουν τα παρακάτω:
Ο Ανάδοχος συναινεί στο πλαίσιο της διαδικασίας εκτέλεσης της παρούσας δημόσιας σύμβασης και επιτρέπει στην Αναθέτουσα Αρχή να προβεί σε αναζήτηση-επιβεβαίωση όλων των αναγκαίων δικαιολογητικών, καθώς και στην αναγκαία επεξεργασία και διατήρηση δεδομένων προσωπικού χαρακτήρα και στην ανταλλαγή πληροφοριών με άλλες δημόσιες αρχές.

Η Αναθέτουσα Αρχή αποθηκεύει και επεξεργάζεται τα στοιχεία προσωπικών δεδομένων του Αναδόχου που είναι αναγκαία για την εκτέλεση της σύμβασης, την εκπλήρωση των μεταξύ τους συναλλαγών και την εν γένει συμμόρφωσή της με νόμιμη υποχρέωση, σε έγχαρτο αρχείο και σε ηλεκτρονική βάση με υψηλά χαρακτηριστικά ασφαλείας με πρόσβαση αυστηρώς και μόνο σε εξουσιοδοτημένα πρόσωπα ή παρόχους υπηρεσιών στους οποίους αναθέτει την εκτέλεση συγκεκριμένων εργασιών για λογαριασμό της και οι οποίοι διενεργούν πράξεις επεξεργασίας προσωπικών δεδομένων.

Η Αναθέτουσα Αρχή θα προβεί σε συλλογή και επεξεργασία (π.χ. συλλογή, καταχώριση, οργάνωση, αποθήκευση, μεταβολή, διαγραφή, καταστροφή κ.λπ.), για τους ανωτέρω αναφερόμενους σκοπούς, των δεδομένων προσωπικού χαρακτήρα όπως: (α) επίσημων στοιχείων ταυτοποίησης, (β) στοιχείων επικοινωνίας, (γ) δεδομένων και πληροφοριών κοινωνικοασφαλιστικών και φορολογικών απαιτήσεων, (δ) γενικών πληροφοριών, (ε) στοιχείων πληρωμής, χρηματοοικονομικών πληροφοριών και λογαριασμών, (στ) δεδομένων ειδικής κατηγορίας, των οποίων η συλλογή και επεξεργασία επιβάλλεται από τους όρους εκτέλεσης της σύμβασης, σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, ή στατιστικούς σκοπούς.

Τα προσωπικά δεδομένα του Αναδόχου και των συνεργατών του (συμπεριλαμβανομένων των δανειζόντων εμπειρία/υπεργολάβων) αποθηκεύονται για χρονικό διάστημα ίσο με τη διάρκεια της εκτέλεσης της σύμβασης, και μετά τη λήξη αυτής για χρονικό διάστημα πέντε ετών για μελλοντικούς φορολογικούς-

δημοσιονομικούς ή ελέγχους χρηματοδοτών ή άλλους προβλεπόμενους ελέγχους από την κείμενη νομοθεσία, εκτός εάν η νομοθεσία προβλέπει διαφορετική περίοδο διατήρησης. Σε περίπτωση εκκρεμοδικίας αναφορικά με δημόσια σύμβαση τα δεδομένα τηρούνται μέχρι το πέρας της εκκρεμοδικίας.

Καθ' όλη την διάρκεια που η Αναθέτουσα Αρχή τηρεί και επεξεργάζεται τα προσωπικά δεδομένα ο Ανάδοχος έχει δικαίωμα ενημέρωσης, πρόσβασης, φορητότητας, διόρθωσης, περιορισμού, διαγραφής ή και εναντίωσης υπό συγκεκριμένες προϋποθέσεις προβλεπόμενες από το νομοθετικό πλαίσιο.

Δεν επιτρέπεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπό διαφορετικό από αυτόν για τον οποίο έχουν συλλεχθεί παρά μόνον υπό τους όρους και προϋποθέσεις του άρθρου 24 του ν. 4624/2019.

Η διαβίβαση δεδομένων προσωπικού χαρακτήρα από την Αναθέτουσα Αρχή σε άλλο δημόσιο φορέα επιτρέπεται σύμφωνα με το άρθρο 26 του ως άνω νόμου, εφόσον είναι απαραίτητο για την εκτέλεση των καθηκόντων της ή του τρίτου φορέα στον οποίο διαβιβάζονται τα δεδομένα και εφόσον πληρούνται οι προϋποθέσεις που επιτρέπουν την επεξεργασία σύμφωνα με το άρθρο 24 του ίδιου νόμου.
Τα στοιχεία επικοινωνίας με τον υπεύθυνο για την προστασία των προσωπικών δεδομένων της Αναθέτουσας Αρχής είναι τα ακόλουθα (email dpo@mykonos.gr).

Β. Ως προς την επεξεργασία από τον ανάδοχο προσωπικών δεδομένων στο πλαίσιο εκτέλεσης των συμβατικών του υποχρεώσεων ισχύουν οι διατάξεις του άρθρου 28 ΓΚΠΔ. Ειδικότερα, ισχύουν τα παρακάτω:
α) ο ανάδοχος (εκτελών την επεξεργασία) επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών της αναθέτουσας αρχής (υπεύθυνος επεξεργασίας),
β) διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή τελούν υπό τη δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας,
γ) λαμβάνει όλα τα απαιτούμενα μέτρα δυνάμει του άρθρου 32 ΓΚΠΔ,
δ) τηρεί τους όρους που αναφέρονται στις παραγράφους 2 και 4 για την πρόσληψη άλλου εκτελούντος την επεξεργασία,
ε) λαμβάνει υπόψη τη φύση της επεξεργασίας και επικουρεί τον υπεύθυνο επεξεργασίας με τα κατάλληλα τεχνικά και οργανωτικά μέτρα, στον βαθμό που αυτό είναι δυνατό, για την εκπλήρωση της υποχρέωσης του υπευθύνου επεξεργασίας να απαντά σε αιτήματα για άσκηση των προβλεπόμενων στο κεφάλαιο ΙΙΙ δικαιωμάτων του υποκειμένου των δεδομένων,
στ) συνδράμει τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις υποχρεώσεις που απορρέουν από τα άρθρα 32 έως 36 ΓΚΠΔ, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και τις πληροφορίες που διαθέτει ο εκτελών την επεξεργασία,
ζ) κατ' επιλογή του υπευθύνου επεξεργασίας (αναθέτουσα αρχή), διαγράφει ή επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα στον υπεύθυνο επεξεργασίας μετά το πέρας της παροχής υπηρεσιών επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα, εκτός εάν το δίκαιο της Ένωσης ή του κράτους μέλους απαιτεί την αποθήκευση των δεδομένων προσωπικού χαρακτήρα,

η) θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις που θεσπίζονται στο παρόν άρθρο και επιτρέπει και διευκολύνει τους ελέγχους, περιλαμβανομένων των επιθεωρήσεων, που διενεργούνται από τον υπεύθυνο επεξεργασίας ή από άλλον ελεγκτή εντεταλμένο από τον υπεύθυνο επεξεργασίας.

ι) Ο εκτελών την επεξεργασία δεν προσλαμβάνει άλλον εκτελούντα την επεξεργασία χωρίς προηγούμενη ειδική ή γενική γραπτή άδεια του υπευθύνου επεξεργασίας.

Αυτά δήλωσαν, συνομολόγησαν και συναποδέχτηκαν οι δύο συμβαλλόμενοι και για τον λόγο αυτό συνέταξαν το παρόν συμφωνητικό σε τρία (3) αντίγραφα που υπογράφεται ως ακολούθως:

ΟΙ ΣΥΜΒΑΛΛΟΜΕΝΟΙ

Για τον Δήμο Μυκόνου

Ο ΔΗΜΑΡΧΟΣ ΜΥΚΟΝΟΥ
CHRISTOS VERONIS
31/12/2025 11:16
ΒΕΡΩΝΗΣ Γ. ΧΡΗΣΤΟΣ

Για την PUBLIC AUDIT SERVICES ΕΕ

Η ΝΟΜΙΜΗ ΕΚΠΡΟΣΩΠΟΣ

ΑΝΝΑ ΣΥΡΡΗ

ANNA SYRRI
Digitally signed by ANNA SYRRI
Date: 2025.12.31 09:50:59 +02'00'

ΠΑΡΑΡΤΗΜΑ
ΣΥΜΒΑΣΗ ΕΠΕΞΕΡΓΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Α. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα πραγματοποιείται σύμφωνα με τις διατάξεις της ισχύουσας ενωσιακής νομοθεσίας και της εκάστοτε ισχύουσας νομοθεσίας κράτους-μέλους για την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως τον Κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (στο εξής: **ΓΚΠΔ**), τη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης, καθώς και τις Αποφάσεις, Γνωμοδοτήσεις και Κατευθυντήριες γραμμές του Ευρωπαϊκού Συμβούλιου Προστασίας Δεδομένων (στο εξής: **Εφαρμοστέα Νομοθεσία για την Προστασία Προσωπικών Δεδομένων**).
Β. Ο υπεύθυνος επεξεργασίας έχει καθορίσει τους σκοπούς και τα μέσα επεξεργασίας προσωπικών δεδομένων σύμφωνα με την υπ.αρ.: 32147 Σύμβαση Συνεργασίας – Ετήσια Παροχή Ανεξάρτητων Υπηρεσιών Υποστήριξης της **Υπηρεσίας Εσωτερικού Ελέγχου** στην οποία επισυνάπτεται η παρούσα.
Γ. Ο εκτελών την επεξεργασία θα συλλέγει, αποθηκεύει και εν γένει επεξεργάζεται προσωπικά δεδομένα για λογαριασμό και σύμφωνα με τις εντολές και οδηγίες του υπευθύνου επεξεργασίας στο πλαίσιο εκτέλεσης της Σύμβασης Συνεργασίας - Παροχής Υπηρεσιών.
Δ. Όπου στο παρόν χρησιμοποιούνται έννοιες που ορίζονται στον Γενικό Κανονισμό Προστασίας Δεδομένων, αυτές έχουν την έννοια που αποδίδεται σε αυτές στον ΓΚΠΔ.

Τα μέρη συμφώνησαν και αποδέχθηκαν τη σύναψη αυτού του Παραρτήματος για την εκτέλεση της Σύμβασης Συνεργασίας - Παροχής Υπηρεσιών, ως εξής:

ΤΜΗΜΑ Ι

Ρήτρα 1
Σκοπός και πεδίο εφαρμογής

α) Οι παρούσες συμβατικές ρήτρες (στο εξής: **ρήτρες**) έχουν ως σκοπό να διασφαλίζουν τη συμμόρφωση με το άρθρο 28 παρ. 3 και 4 του Κανονισμού (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 των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ.

β) Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία που ορίζονται στο Προσάρτημα Ι συμφώνησαν τις παρούσες ρήτρες προκειμένου να διασφαλίζεται η συμμόρφωση με το άρθρο 28 παράγραφοι 3 και 4 του ΓΚΠΔ.

γ) Οι παρούσες ρήτρες εφαρμόζονται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα όπως καθορίζεται στο Προσάρτημα ΙΙ.

δ) Τα προσαρτήματα Ι έως ΙV είναι αναπόσπαστο μέρος των ρητρών.

ε) Οι παρούσες ρήτρες δεν θίγουν τις υποχρεώσεις στις οποίες υπόκειται ο υπεύθυνος επεξεργασίας δυνάμει του ΓΚΠΔ.

στ) Οι παρούσες ρήτρες δεν διασφαλίζουν από μόνες τους τη συμμόρφωση με τις υποχρεώσεις που σχετίζονται με τις διεθνείς διαβιβάσεις σύμφωνα με το κεφάλαιο V του ΓΚΠΔ.

ζ) Τυχόν ακυρότητα οποιασδήποτε ρήτρας του παρόντος δεν επηρεάζει την ισχύ των λοιπών, το δε παράρτημα συνεχίζει να ισχύει στο σύνολό του χωρίς την εν λόγω άκυρη ρήτρα.

Ρήτρα 2
Αμετάβλητος χαρακτήρας των ρητρών

α) Τα μέρη δεσμεύονται να μην τροποποιούν τις ρήτρες παρά μόνο για να προσθέσουν ή να επικαιροποιήσουν πληροφορίες στα προσαρτήματα.

β) Η δέσμευση αυτή δεν εμποδίζει τα μέρη να ενσωματώνουν τις παρούσες συμβατικές ρήτρες σε ευρύτερη σύμβαση ούτε να προσθέτουν άλλες ρήτρες ή πρόσθετες εγγυήσεις,

υπό τον όρο ότι αυτές δεν αντιφάσκουν, άμεσα ή έμμεσα, προς τις ρήτρες ούτε θίγουν τα θεμελιώδη δικαιώματα ή τις ελευθερίες των υποκειμένων των δεδομένων.

Ρήτρα 3

Ερμηνεία

α) Όπου στις παρούσες ρήτρες χρησιμοποιούνται όροι που ορίζονται στον ΓΚΠΔ, οι εν λόγω όροι έχουν την ίδια έννοια με αυτή που έχουν στον οικείο κανονισμό.

β) Η ανάγνωση και ερμηνεία των παρουσών ρητρών πραγματοποιούνται υπό το πρίσμα των διατάξεων της Εφαρμοστέας Νομοθεσίας για την Προστασία Προσωπικών Δεδομένων.

γ) Οι παρούσες ρήτρες δεν ερμηνεύονται με τρόπο που αντιβαίνει προς τα δικαιώματα και τις υποχρεώσεις που προβλέπονται στην Εφαρμοστέα Νομοθεσία για την Προστασία Προσωπικών Δεδομένων ή με τρόπο που θίγει τα θεμελιώδη δικαιώματα ή τις ελευθερίες των υποκειμένων των δεδομένων.

Ρήτρα 4

Ιεραρχία

Σε περίπτωση αντίφασης μεταξύ των παρουσών ρητρών και των διατάξεων συναφών συμφωνιών μεταξύ των μερών οι οποίες ισχύουν κατά τον χρόνο που συμφωνούνται ή συνάπτονται οι παρούσες ρήτρες, οι παρούσες ρήτρες υπερισχύουν.

ΤΜΗΜΑ ΙΙ – ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΣΥΜΒΑΛΛΟΜΕΝΩΝ ΜΕΡΩΝ

Ρήτρα 5

Περιγραφή της επεξεργασίας

Οι λεπτομέρειες των πράξεων επεξεργασίας, ιδίως οι κατηγορίες των δεδομένων προσωπικού χαρακτήρα και οι σκοποί της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας, καθορίζονται στο Προσάρτημα ΙΙ.

Ρήτρα 6

Υποχρεώσεις των συμβαλλόμενων μερών

6.1. Εντολές

α) Ο εκτελών την επεξεργασία επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας, εκτός εάν υποχρεούται προς τούτο βάσει του δικαίου της Ένωσης ή του δικαίου του κράτους μέλους στο οποίο υπόκειται ο εκτελών την επεξεργασία. Στην περίπτωση αυτή, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας για την εν λόγω νομική απαίτηση πριν από την επεξεργασία, εκτός εάν το εν λόγω δίκαιο απαγορεύει αυτού του είδους την ενημέρωση για σοβαρούς λόγους δημόσιου συμφέροντος. Ο υπεύθυνος επεξεργασίας μπορεί επίσης να δίνει μεταγενέστερες εντολές καθ' όλη τη διάρκεια της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα. Οι εν λόγω εντολές είναι πάντοτε έγγραφες.

β) Ο εκτελών την επεξεργασία ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας, εάν, κατά την άποψη του εκτελούντος της επεξεργασία, κάποια εντολή του υπευθύνου επεξεργασίας παραβιάζει την Εφαρμοστέα Νομοθεσία για την Προστασία Προσωπικών Δεδομένων ή ενωσιακές ή εθνικές διατάξεις περί προστασίας δεδομένων. Ρητά συμφωνείται δια του παρόντος ότι ο εκτελών την επεξεργασία δεν έχει υποχρέωση να ελέγχει τη νομιμότητα κάθε εντολής που δίνεται από τον υπεύθυνο επεξεργασίας.

6.2. Περιορισμός του σκοπού

Ο εκτελών την επεξεργασία επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα μόνο για τον συγκεκριμένο σκοπό ή σκοπούς της επεξεργασίας που ορίζονται στο Προσάρτημα ΙΙ, εκτός αν λάβει περαιτέρω εντολές από τον υπεύθυνο επεξεργασίας.

6.3. Διάρκεια της επεξεργασίας δεδομένων προσωπικού χαρακτήρα

Η επεξεργασία από τον εκτελούντα την επεξεργασία πραγματοποιείται μόνο για το χρονικό διάστημα που καθορίζεται στο Προσάρτημα ΙΙ.

6.4. Ασφάλεια της επεξεργασίας

α) Ο εκτελών την επεξεργασία εφαρμόζει τουλάχιστον τα τεχνικά και οργανωτικά μέτρα που καθορίζονται στο Προσάρτημα ΙΙΙ προκειμένου να διασφαλίζει την ασφάλεια των δεδομένων προσωπικού χαρακτήρα. Στο πλαίσιο αυτό συμπεριλαμβάνεται η προστασία των δεδομένων από παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ αδείας κοινολόγηση ή προσπέλαση δεδομένων (στο εξής: **παραβίαση δεδομένων προσωπικού χαρακτήρα**). Κατά την αξιολόγηση του κατάλληλου επιπέδου ασφάλειας, τα συμβαλλόμενα μέρη λαμβάνουν δεόντως υπόψη τις τελευταίες εξελίξεις, το κόστος εφαρμογής, τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, καθώς και τους κινδύνους που συντρέχουν για τα υποκείμενα των δεδομένων.

β) Ο εκτελών την επεξεργασία παρέχει σε μέλη του προσωπικού του πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία μόνο στο μέτρο που είναι απολύτως αναγκαίο για την εκτέλεση, τη διαχείριση και την παρακολούθηση της Σύμβασης Συνεργασίας -Παροχής Υπηρεσιών. Ο εκτελών την επεξεργασία διασφαλίζει ότι τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα έχουν αναλάβει δέσμευση τήρησης εμπιστευτικότητας ή υπόκεινται σε δέουσα κανονιστική υποχρέωση τήρησης εμπιστευτικότητας.

6.5. Δεδομένα ειδικής κατηγορίας

Αν η επεξεργασία περιλαμβάνει δεδομένα προσωπικού χαρακτήρα ειδικών κατηγοριών (στο εξής: **ευαίσθητα δεδομένα**), ο εκτελών την επεξεργασία εφαρμόζει ειδικούς περιορισμούς και/ή πρόσθετες εγγυήσεις.

6.6 Τεκμηρίωση και συμμόρφωση

α) Τα συμβαλλόμενα μέρη είναι σε θέση να αποδείξουν τη συμμόρφωσή τους με τις παρούσες ρήτρες.

β) Ο εκτελών την επεξεργασία ανταποκρίνεται άμεσα και επαρκώς σε όλα τα αιτήματα πληροφοριών του υπευθύνου επεξεργασίας σχετικά με την επεξεργασία δεδομένων σύμφωνα με τις παρούσες ρήτρες.

γ) Ο εκτελών την επεξεργασία θέτει στη διάθεση του υπευθύνου επεξεργασίας κάθε απαραίτητη πληροφορία προς απόδειξη της συμμόρφωσης προς τις υποχρεώσεις που καθορίζονται στις παρούσες ρήτρες και απορρέουν απευθείας από τον ΓΚΠΔ. Επιπλέον, κατόπιν αιτήματος του υπευθύνου επεξεργασίας, ο εκτελών την επεξεργασία επιτρέπει και διευκολύνει ελέγχους των δραστηριοτήτων επεξεργασίας που καλύπτονται από τις παρούσες ρήτρες, σε εύλογα τακτά χρονικά διαστήματα ή αν υπάρχουν ενδείξεις μη συμμόρφωσης. Όταν αποφασίζει για επανεξέταση ή έλεγχο, ο υπεύθυνος επεξεργασίας μπορεί να λαμβάνει υπόψη σχετικές πιστοποιήσεις του εκτελούντος την επεξεργασία.

δ) Ο υπεύθυνος επεξεργασίας μπορεί να επιλέγει να διενεργήσει τον έλεγχο ο ίδιος ή να τον αναθέσει σε ανεξάρτητο ελεγκτή. Οι έλεγχοι είναι δυνατόν να περιλαμβάνουν και επιθεωρήσεις στους χώρους ή τις φυσικές εγκαταστάσεις του εκτελούντος την επεξεργασία, ενώ, όταν ενδείκνυται, διενεργούνται έπειτα από εύλογη προθεσμία προειδοποίησης.

ε) Τα συμβαλλόμενα μέρη θέτουν τις πληροφορίες που αναφέρονται στην παρούσα ρήτρα, συμπεριλαμβανομένων των αποτελεσμάτων τυχόν ελέγχων, στη διάθεση της/των αρμόδιας/-ων εποπτικής/-ών αρχής/-ών, κατόπιν σχετικού αιτήματός της/τους.

6.7. Χρήση υπεργολάβων επεξεργασίας

α) Ο εκτελών την επεξεργασία έχει τη γενική άδεια του υπευθύνου επεξεργασίας για την πρόσληψη υπεργολάβων επεξεργασίας από κατάλογο που έχει συμφωνηθεί και παρατίθεται στο Προσάρτημα IV του παρόντος. Ο εκτελών την επεξεργασία ενημερώνει ειδικά και εγγράφως τον υπεύθυνο επεξεργασίας για κάθε τυχόν σκοπούμενη αλλαγή στον εν λόγω κατάλογο η οποία αφορά την προσθήκη ή την αντικατάσταση

υπεργολάβων επεξεργασίας τουλάχιστον δέκα (10) ημέρες πριν, παρέχοντας στον υπεύθυνο επεξεργασίας επαρκή χρόνο ώστε να μπορέσει να εναντιωθεί στην εν λόγω αλλαγή πριν από την πρόσληψη του σχετικού υπεργολάβου ή των σχετικών υπεργολάβων επεξεργασίας. Ο εκτελών την επεξεργασία παρέχει στον υπεύθυνο επεξεργασίας τις πληροφορίες που απαιτούνται ώστε ο τελευταίος να είναι σε θέση να ασκήσει το δικαίωμα εναντίωσης. Η μη εναντίωση του υπευθύνου επεξεργασίας στη σκοπούμενη αλλαγή, εντός της ως άνω προθεσμίας, λογίζεται ως αποδοχή αυτής.

β) Όταν ο εκτελών την επεξεργασία προσλαμβάνει υπεργολάβο επεξεργασίας, που δεν περιλαμβάνεται στο Προσάρτημα IV, για την εκτέλεση συγκεκριμένων δραστηριοτήτων επεξεργασίας (για λογαριασμό του υπευθύνου επεξεργασίας), το πράττει μέσω σύμβασης η οποία επιβάλλει στον υπεργολάβο επεξεργασίας, στην ουσία, τις ίδιες υποχρεώσεις όσον αφορά την προστασία των δεδομένων με αυτές που επιβάλλονται στον εκτελούντα την επεξεργασία σύμφωνα με το παρόν και κατόπιν αιτήματος του υπευθύνου επεξεργασίας παρέχει σε αυτόν αντίγραφο της συμφωνίας με τον υπεργολάβο και κάθε τυχόν μεταγενέστερης πράξης τροποποίησής της. Ο εκτελών την επεξεργασία διασφαλίζει ότι ο υπεργολάβος επεξεργασίας συμμορφώνεται με τις υποχρεώσεις στις οποίες υπόκειται ο εκτελών την επεξεργασία σύμφωνα με το παρόν και τον ΓΚΠΔ.

γ) Ο εκτελών την επεξεργασία παραμένει υπεύθυνος έναντι του υπευθύνου επεξεργασίας για την εκπλήρωση των υποχρεώσεων του υπεργολάβου επεξεργασίας σύμφωνα με τη σύμβασή του με τον εκτελούντα την επεξεργασία.

6.8. Διεθνείς διαβιβάσεις

α) Κάθε διαβίβαση δεδομένων σε τρίτη χώρα ή διεθνή οργανισμό από τον εκτελούντα την επεξεργασία πραγματοποιείται μόνο βάσει καταγεγραμμένων εντολών του υπευθύνου επεξεργασίας ή προκειμένου να εκπληρωθεί ειδική απαίτηση του δικαίου της Ένωσης ή του κράτους μέλους στο οποίο υπόκειται ο εκτελών την επεξεργασία και εκτελείται σύμφωνα με τους όρους του κεφαλαίου V του ΓΚΠΔ.

β) Ο υπεύθυνος επεξεργασίας συμφωνεί ότι στις περιπτώσεις που ο εκτελών την επεξεργασία προσλαμβάνει υπεργολάβο επεξεργασίας σύμφωνα με τη ρήτρα 6.7 για την εκτέλεση συγκεκριμένων δραστηριοτήτων επεξεργασίας (για λογαριασμό του υπευθύνου επεξεργασίας) και οι εν λόγω δραστηριότητες επεξεργασίας περιλαμβάνουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα κατά την έννοια του κεφαλαίου V του ΓΚΠΔ, ο εκτελών την επεξεργασία και ο υπεργολάβος επεξεργασίας μπορούν να διασφαλίζουν τη συμμόρφωση με το κεφάλαιο V του ΓΚΠΔ μέσω της χρήσης τυποποιημένων συμβατικών ρητρών που έχει εκδώσει η Επιτροπή σύμφωνα με το άρθρο 46 παρ. 2 του ΓΚΠΔ, υπό τον όρο ότι πληρούνται οι προϋποθέσεις για τη χρήση των εν λόγω τυποποιημένων συμβατικών ρητρών.

6.9 Δηλώσεις και εγγυήσεις του υπευθύνου επεξεργασίας

α) Ο υπεύθυνος επεξεργασίας, δηλώνει και εγγυάται ότι επεξεργάζεται τα δεδομένα προσωπικού χαρακτήρα σύμφωνα με την Εφαρμοστέα Νομοθεσία για την Προστασία Δεδομένων. Ειδικότερα, ο υπεύθυνος επεξεργασίας δηλώνει και εγγυάται ότι έχει ενημερώσει τα υποκείμενα των δεδομένων σύμφωνα με τα άρθρα 13 ή 14 ΓΚΠΔ και έχει λάβει τη συγκατάθεσή τους, εφόσον απαιτείται, καθώς επίσης και ότι είναι ο μοναδικός υπεύθυνος επεξεργασίας που καθορίζει μόνος το σκοπό και τον τρόπο της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

β) Ο υπεύθυνος επεξεργασίας δηλώνει ότι ο εκτελών την επεξεργασία παρέχει επαρκείς διαβεβαιώσεις για την εφαρμογή κατάλληλων τεχνικών και οργανωτικών μέτρων κατά τρόπο ώστε η επεξεργασία να πληροί τις απαιτήσεις του ΓΚΠΔ και να διασφαλίζεται η προστασία των δικαιωμάτων και ελευθεριών των υποκειμένων των δεδομένων. Ο υπεύθυνος επεξεργασίας δηλώνει ότι με την υπογραφή του παρόντος εγκρίνει τα τεχνικά και οργανωτικά μέτρα του Προσαρτήματος ΙΙΙ ως κατάλληλα και επαρκή για την εξασφάλιση επαρκούς επιπέδου προστασίας των δεδομένων προσωπικού χαρακτήρα, λαμβάνοντας υπόψη τη φύση και το σκοπό της επεξεργασίας, το κόστος εφαρμογής καθώς και τους κινδύνους για τα υποκείμενα των δεδομένων.

Ρήτρα 7

Συνδρομή στον υπεύθυνο επεξεργασίας

α) Ο εκτελών την επεξεργασία ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας για κάθε αίτημα που έχει λάβει από υποκείμενο των δεδομένων. Δεν απαντά ο ίδιος στο αίτημα, εκτός αν λάβει σχετική εξουσιοδότηση με το περιεχόμενο της απάντησης από τον υπεύθυνο επεξεργασίας.

β) Ο εκτελών την επεξεργασία βοηθά τον υπεύθυνο επεξεργασίας στην εκπλήρωση της υποχρέωσής του να απαντά στα αιτήματα των υποκειμένων των δεδομένων για άσκηση των δικαιωμάτων τους, λαμβανομένης υπόψη της φύσης της επεξεργασίας. Κατά την εκπλήρωση των υποχρεώσεών του σύμφωνα με τα στοιχεία α) και β), ο εκτελών την επεξεργασία συμμορφώνεται με τις εντολές του υπευθύνου επεξεργασίας.

γ) Επιπρόσθετα στην υποχρέωση του εκτελούντος την επεξεργασία να βοηθά τον υπεύθυνο επεξεργασίας σύμφωνα με τη ρήτρα 7 στοιχείο β), ο εκτελών την επεξεργασία βοηθά επίσης τον υπεύθυνο επεξεργασίας στη διασφάλιση της συμμόρφωσης προς τις παρακάτω υποχρεώσεις, λαμβανομένων υπόψη της φύσης της επεξεργασίας δεδομένων και των πληροφοριών που διαθέτει ο εκτελών την επεξεργασία:

1) την υποχρέωση να διενεργεί εκτίμηση του αντικτύπου των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία των δεδομένων προσωπικού χαρακτήρα (εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων), όταν ένα είδος επεξεργασίας ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων·

2) την υποχρέωση να ζητεί τη γνώμη της/των αρμόδιας/-ων εποπτικής/-ών αρχής/-ών πριν από την επεξεργασία, όταν μια εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων υποδεικνύει ότι η επεξεργασία θα προκαλούσε υψηλό κίνδυνο ελλείψει μέτρων μετριασμού του κινδύνου από τον υπεύθυνο επεξεργασίας·

3) την υποχρέωση να διασφαλίζει ότι τα δεδομένα προσωπικού χαρακτήρα είναι ακριβή και επικαιροποιημένα, ενημερώνοντας χωρίς καθυστέρηση τον υπεύθυνο επεξεργασίας σε περίπτωση που ο εκτελών την επεξεργασία αντιληφθεί ότι τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται είναι ανακριβή ή παρωχημένα·

4) τις υποχρεώσεις που προβλέπονται στο άρθρο 32 του ΓΚΠΔ.

δ) Τα συμβαλλόμενα μέρη καθορίζουν στο Προσάρτημα ΙΙΙ τα κατάλληλα τεχνικά και οργανωτικά μέτρα με τα οποία ο εκτελών την επεξεργασία υποχρεούται να βοηθά τον υπεύθυνο επεξεργασίας για την εφαρμογή της παρούσας ρήτρας, καθώς και το πεδίο εφαρμογής και την έκταση της απαιτούμενης βοήθειας.

Ρήτρα 8

Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο εκτελών την επεξεργασία συνεργάζεται με τον υπεύθυνο επεξεργασίας και τον βοηθά να συμμορφωθεί προς τις υποχρεώσεις του που απορρέουν από τα άρθρα 33 και 34 του ΓΚΠΔ, ανάλογα με την περίπτωση, λαμβανομένων υπόψη της φύσης της επεξεργασίας και των πληροφοριών που διαθέτει ο εκτελών την επεξεργασία.

8.1 Παραβίαση δεδομένων που αφορά δεδομένα που επεξεργάζεται ο υπεύθυνος επεξεργασίας

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που αφορά δεδομένα που επεξεργάζεται ο υπεύθυνος επεξεργασίας, ο εκτελών την επεξεργασία βοηθά τον υπεύθυνο επεξεργασίας:

α) να γνωστοποιήσει την παραβίαση δεδομένων προσωπικού χαρακτήρα στην/στις αρμόδια/-ες εποπτική/-ές αρχή/-ές, αμελλητί από τη στιγμή που ο υπεύθυνος επεξεργασίας απέκτησε γνώση του γεγονότος, κατά περίπτωση/(εκτός αν η παραβίαση

δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων)·

β) να συγκεντρώσει τις παρακάτω πληροφορίες, οι οποίες, σύμφωνα με το άρθρο 33 παρ. 3 του ΓΚΠΔ, αναφέρονται στη γνωστοποίηση του υπευθύνου επεξεργασίας και πρέπει να περιλαμβάνουν κατ' ελάχιστο:

1) τη φύση των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων, όπου είναι δυνατό, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων, καθώς και των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων αρχείων δεδομένων προσωπικού χαρακτήρα·

2) τις ενδεχόμενες συνέπειες της παραβίασης των δεδομένων προσωπικού χαρακτήρα·

3) τα ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Όταν και στον βαθμό που δεν είναι δυνατόν να παρασχεθούν όλες αυτές οι πληροφορίες ταυτόχρονα, στην αρχική γνωστοποίηση περιλαμβάνονται οι πληροφορίες που είναι διαθέσιμες τη δεδομένη στιγμή, ενώ πρόσθετες πληροφορίες παρέχονται σε μεταγενέστερο χρόνο και χωρίς αδικαιολόγητη καθυστέρηση μόλις καταστούν διαθέσιμες.

γ) να συμμορφωθεί, σύμφωνα με το άρθρο 34 του ΓΚΠΔ, με την υποχρέωση να ανακοινώνει αμελλητί στο υποκείμενο των δεδομένων την παραβίαση δεδομένων προσωπικού χαρακτήρα, όταν αυτή ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

8.2 Παραβίαση δεδομένων που αφορά δεδομένα που επεξεργάζεται ο εκτελών την επεξεργασία

Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα που αφορά δεδομένα που επεξεργάζεται ο εκτελών την επεξεργασία, ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση από τη στιγμή που αποκτά γνώση της παραβίασης. Η εν λόγω γνωστοποίηση περιλαμβάνει κατ' ελάχιστο:

α) περιγραφή της φύσης της παραβίασης (συμπεριλαμβανομένων, όπου είναι δυνατόν, των κατηγοριών και του κατά προσέγγιση αριθμού των επηρεαζόμενων υποκειμένων των δεδομένων και αρχείων δεδομένων)·

β) τα στοιχεία του σημείου επικοινωνίας από το οποίο μπορούν να ληφθούν περισσότερες πληροφορίες σχετικά με την παραβίαση των δεδομένων προσωπικού χαρακτήρα·

γ) τις ενδεχόμενες συνέπειες και τα ληφθέντα ή προτεινόμενα προς λήψη μέτρα για την αντιμετώπιση της παραβίασης, καθώς και, όπου ενδείκνυται, μέτρα για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της.

Όταν και στον βαθμό που δεν είναι δυνατόν να παρασχεθούν όλες αυτές οι πληροφορίες ταυτόχρονα, στην αρχική γνωστοποίηση περιλαμβάνονται οι πληροφορίες που είναι διαθέσιμες τη δεδομένη στιγμή, ενώ πρόσθετες πληροφορίες παρέχονται σε μεταγενέστερο χρόνο και χωρίς αδικαιολόγητη καθυστέρηση μόλις καταστούν διαθέσιμες.

Τα συμβαλλόμενα μέρη καθορίζουν στο Προσάρτημα ΙΙΙ όλα τα άλλα στοιχεία που πρέπει να παρέχονται από τον εκτελούντα την επεξεργασία κατά την παροχή βοήθειας στον υπεύθυνο επεξεργασίας για τη συμμόρφωση προς τις υποχρεώσεις του υπευθύνου επεξεργασίας σύμφωνα με τα άρθρα 33 και 34 του ΓΚΠΔ.

ΤΜΗΜΑ ΙΙΙ – ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Ρήτρα 9

Μη συμμόρφωση με τις ρήτρες και καταγγελία

α) Με την επιφύλαξη των διατάξεων του ΓΚΠΔ, σε περίπτωση που ο εκτελών την επεξεργασία παραβιάζει τις υποχρεώσεις του σύμφωνα με τις παρούσες ρήτρες, ο υπεύθυνος επεξεργασίας μπορεί να δώσει εντολή στον εκτελούντα την επεξεργασία να αναστείλει την επεξεργασία δεδομένων προσωπικού χαρακτήρα έως ότου ο τελευταίος συμμορφωθεί με τις παρούσες ρήτρες ή καταγγελθεί η Σύμβαση Συνεργασίας –

Παροχής Υπηρεσιών. Ο εκτελών την επεξεργασία ενημερώνει αμέσως τον υπεύθυνο επεξεργασίας σε περίπτωση που αδυνατεί να συμμορφωθεί με τις παρούσες ρήτρες, για οποιονδήποτε λόγο.

β) Ο υπεύθυνος επεξεργασίας έχει δικαίωμα να καταγγείλει τη Σύμβαση στον βαθμό που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις παρούσες ρήτρες, αν:

1) η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τον εκτελούντα την επεξεργασία ανεστάλη από τον υπεύθυνο επεξεργασίας σύμφωνα με το στοιχείο α) και η συμμόρφωση με τις παρούσες ρήτρες δεν αποκαταστάθηκε εντός εύλογου χρονικού διαστήματος και, σε κάθε περίπτωση, εντός ενός μηνός από την ημερομηνία της αναστολής·

2) ο εκτελών την επεξεργασία παραβιάζει ουσιωδώς ή με τρόπο διαρκή τις παρούσες ρήτρες ή τις υποχρεώσεις του βάσει του ΓΚΠΔ ή της Εφαρμοστέας Νομοθεσίας για την Προστασία Προσωπικών Δεδομένων·

3) ο εκτελών την επεξεργασία δεν συμμορφώνεται με δεσμευτική απόφαση αρμόδιου δικαστηρίου ή της/των αρμόδιας/-ων εποπτικής/-ών αρχής/-ών όσον αφορά τις υποχρεώσεις του σύμφωνα με τις παρούσες ρήτρες ή την Εφαρμοστέα Νομοθεσία για την Προστασία Προσωπικών Δεδομένων.

γ) Ο εκτελών την επεξεργασία έχει δικαίωμα να καταγγείλει τη Σύμβαση Συνεργασίας – Παροχής Υπηρεσιών στον βαθμό που αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις παρούσες ρήτρες αν, παρόλο που έχει ενημερώσει τον υπεύθυνο επεξεργασίας ότι οι εντολές του παραβιάζουν εφαρμοστέες νομικές απαιτήσεις σύμφωνα με τη ρήτρα 6.1 στοιχείο β), ο υπεύθυνος επεξεργασίας εμμένει στη συμμόρφωση με τις εν λόγω εντολές.

δ) Μετά την καταγγελία της Σύμβασης Συνεργασίας – Παροχής Υπηρεσιών, ο εκτελών την επεξεργασία, κατ' επιλογή του υπευθύνου επεξεργασίας, διαγράφει όλα τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζεται για λογαριασμό του υπευθύνου επεξεργασίας και πιστοποιεί στον υπεύθυνο επεξεργασίας ότι το έχει πράξει ή επιστρέφει όλα τα δεδομένα προσωπικού χαρακτήρα στον υπεύθυνο επεξεργασίας και διαγράφει τα υφιστάμενα αντίγραφα, εκτός αν το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους απαιτεί την αποθήκευση των δεδομένων προσωπικού χαρακτήρα. Έως τη διαγραφή ή την επιστροφή των δεδομένων, ο εκτελών την επεξεργασία συνεχίζει να διασφαλίζει τη συμμόρφωση με τις παρούσες ρήτρες.

Ρήτρα 10
Ευθύνη

α) Ο εκτελών την επεξεργασία ευθύνεται πλήρως έναντι του υπευθύνου επεξεργασίας για κάθε άμεση, έμμεση, υφιστάμενη, μελλοντική, θετική ή αποθετική ζημία του τελευταίου εξαιτίας της αθέτησης των υποχρεώσεων που επιβάλλονται δυνάμει της παρούσας ή στις περιπτώσεις που ενήργησε σε αντίθεση με τις εντολές του υπεύθυνου επεξεργασίας. Ομοίως, ευθύνεται κατά τον ίδιο τρόπο αν η εν λόγω ζημία επήλθε ως αποτέλεσμα ή συνέπεια πράξεων ή παραλείψεων των εξουσιοδοτημένων προς επεξεργασία υπαλλήλων ή συνεργατών του ή υπεργολάβων επεξεργασίας.

β) Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία αναλαμβάνει έκαστος όλες τις υποχρεώσεις που ο ΓΚΠΔ ή η Εφαρμοστέα Νομοθεσία για την Προστασία Προσωπικών Δεδομένων προβλέπει και είναι ανεξάρτητα και αυτοτελώς υπεύθυνος για τη συμμόρφωσή του με την ανωτέρω νομοθεσία.

γ) Η πλημμελής ή μη τήρηση των υποχρεώσεων της παρούσας από τον εκτελούντα την επεξεργασία ή από προστηθέντα αυτού ή υπεργολάβο επεξεργασίας για λογαριασμό του, αποτελεί σπουδαίο λόγο καταγγελίας της μεταξύ τους συνεργασίας και της παρούσας σύμβασης.

Ρήτρα 11
Επίλυση Διαφορών

Σε περίπτωση διαφοράς, η οποία απορρέει από την παρούσα, τα συμβαλλόμενα μέρη θα επιδιώξουν την επίλυση αυτής εξώδικα και δια φιλικών διαπραγματεύσεων, αν δε αυτή δεν επιλυθεί εντός δέκα (10) ημερών, δεσμεύονται να συμμετάσχουν σε διαδικασία διαμεσολάβησης εντός προθεσμίας δύο (2) μηνών από την έγερση της διαφοράς. Εάν η διαφορά δεν επιλυθεί μέσα στην παραπάνω προθεσμία, το εφαρμοστέο δίκαιο και τα αρμόδια δικαστήρια ορίζονται στη Σύμβαση Συνεργασίας - Παροχής Υπηρεσιών.

ΠΡΟΣΑΡΤΗΜΑ Ι ΚΑΤΑΛΟΓΟΣ ΣΥΜΒΑΛΛΟΜΕΝΩΝ ΜΕΡΩΝ

Υπεύθυνος Επεξεργασίας: Ο Δήμος, όπως ορίζεται στη Σύμβαση Συνεργασίας - Παροχής Υπηρεσιών

e-mail DPO: dpo@mykonos.gr

Εκτελών την Επεξεργασία: Ο Ανάδοχος, όπως ορίζεται στη Σύμβαση Συνεργασίας - Παροχής Υπηρεσιών

ΠΡΟΣΑΡΤΗΜΑ ΙΙ: ΠΕΡΙΓΡΑΦΗ ΤΗΣ ΕΠΕΞΕΡΓΑΣΙΑΣ

Κατηγορίες υποκειμένων δεδομένων των οποίων τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία

Δεδομένα εργαζομένων και συνεργατών της Αναθέτουσας Αρχής, δεδομένα φυσικών προσώπων νομίμων εκπροσώπων / εργαζομένων / προστηθέντων / συνεργατών / δανειζόντων εμπειρία / υπεργολάβων αντισυμβαλλομένων της Αναθέτουσας Αρχής, δεδομένα δημοτών και πολιτών

Κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία

ταυτοποιητικά δεδομένα και στοιχεία επικοινωνίας των εργαζομένων και συνεργατών της Αναθέτουσας Αρχής,

ταυτοποιητικά δεδομένα, στοιχεία επικοινωνίας και οικονομικά δεδομένα των νομίμων εκπροσώπων / εργαζομένων / προστηθέντων / συνεργατών / δανειζόντων εμπειρία / υπεργολάβων αντισυμβαλλομένων της Αναθέτουσας Αρχής

ταυτοποιητικά δεδομένα και δεδομένα υγείας των ασθενών, ταυτοποιητικά στοιχεία και στοιχεία επικοινωνίας των συνοδών / επισκεπτών.

Ευαίσθητα δεδομένα που υποβάλλονται σε επεξεργασία (αν συντρέχει τέτοια περίπτωση) και περιορισμοί ή εγγυήσεις που εφαρμόζονται ώστε να λαμβάνονται πλήρως υπόψη η φύση των δεδομένων και οι υφιστάμενοι κίνδυνοι, όπως, για παράδειγμα, αυστηρός περιορισμός του σκοπού, περιορισμοί στην πρόσβαση (συμπεριλαμβανομένης της πρόσβασης αποκλειστικά από προσωπικό που έχει λάβει εξειδικευμένη κατάρτιση), τήρηση αρχείου πρόσβασης στα δεδομένα, περιορισμοί στις περαιτέρω διαβιβάσεις ή πρόσθετα μέτρα ασφάλειας.

Δεδομένα υγείας των εργαζομένων με περιορισμό πρόσβασης.

Φύση της επεξεργασίας

Πρόσβαση και προσπέλαση δεδομένων αναγκαία για την παροχή των υπηρεσιών του συμβούλου.

Σκοπός-οί για τον οποίο ή τους οποίους τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία για λογαριασμό του υπευθύνου επεξεργασίας

Ετήσια Παροχή Ανεξάρτητων Υπηρεσιών Υποστήριξης της Υπηρεσίας Εσωτερικού Ελέγχου.

Διάρκεια της επεξεργασίας

Για όσο χρονικό διάστημα προβλέπεται στη σύμβαση συνεργασίας – παροχής υπηρεσιών.

Για την επεξεργασία από εκτελούντες την επεξεργασία (υπεργολάβους επεξεργασίας), να διευκρινιστεί επίσης το αντικείμενο, η φύση και η διάρκεια της επεξεργασίας

(Αναφέρονται στο Προσάρτημα IV)

ΠΡΟΣΑΡΤΗΜΑ ΙΙΙ ΤΕΧΝΙΚΑ ΚΑΙ ΟΡΓΑΝΩΤΙΚΑ ΜΕΤΡΑ, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΩΝ ΤΩΝ ΤΕΧΝΙΚΩΝ ΚΑΙ ΟΡΓΑΝΩΤΙΚΩΝ ΜΕΤΡΩΝ ΓΙΑ ΤΗ ΔΙΑΣΦΑΛΙΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

(συμπλήρωση με √ στα μέτρα που εφαρμόζονται ή σχετίζονται με την επεξεργασία προσωπικών δεδομένων που πραγματοποιείται για λογαριασμό του Δήμου. Η εξειδίκευση των μέτρων είναι ενδεικτική. Να συμπληρωθούν επιπλέον μέτρα εάν υφίστανται)

ΚΑΤΗΓΟΡΙΑ ΜΕΤΡΩΝ	ΕΞΕΙΔΙΚΕΥΣΗ	ΕΦΑΡΜΟΓΗ
Μέτρα ψευδωνυμοποίησης και κρυπτογράφησης δεδομένων προσωπικού χαρακτήρα που αποθηκεύονται στους servers, σε σκληρούς δίσκους υπό μορφή αρχείων ή σε βάσεις δεδομένων	Κατά τη διακίνηση (in transit)	
	Σε επίπεδο συσκευής αποθήκευσης (at rest)	
	Διαδικασίες ψευδωνυμοποίησης και ανά περίπτωση scrambling ή/και data masking για τη πρόσβαση του προσωπικού σε δεδομένα του συστήματος	
Μέτρα για τη διασφάλιση της εμπιστευτικότητας, της ακεραιότητας, της διαθεσιμότητας και της αξιοπιστίας των συστημάτων και των υπηρεσιών επεξεργασίας σε συνεχή βάση	Πολιτική ασφάλειας των συστημάτων δικτύου και πληροφοριών	
	Intrusion Detection (IDS) & Intrusion Prevention Systems (IPS)	
	Περιοδικοί έλεγχοι ασφάλειας	
	Συντήρηση και αναβάθμιση του υλικοτεχνικού εξοπλισμού (hardware) και του λογισμικού (software)	
	Δίκτυο το οποίο προστατεύεται τουλάχιστον με ένα από τα ακόλουθα: IDS/IPS, Firewall	
	Περιοδικοί έλεγχοι ανίχνευσης ιών	
	Data loss prevention policy	
	Δυνατότητα απομόνωσης κρίσιμων στοιχείων πληροφορικής και δικτύου	
	Η εισερχόμενη και εξερχόμενη αλληλογραφία, φιλτράρεται με σύστημα ανίχνευσης ιομορφικού λογισμικού (anti-malware & anti-virus)	
	Χρήση κλειστού δικτύου	
	Απομακρυσμένη επεξεργασία των δεδομένων γίνεται μόνο μέσω VPN/SSL	
Μέτρα για τη διασφάλιση της δυνατότητας αποκατάστασης της διαθεσιμότητας και της πρόσβασης σε δεδομένα προσωπικού χαρακτήρα σε εύθετο χρόνο σε περίπτωση φυσικού ή τεχνικού συμβάντος	Τήρηση κρυπτογραφημένων αντιγράφων ασφαλείας (backups) σε πολλαπλές τοποθεσίες για τα οποία εφαρμόζονται τα ίδια μέτρα ασφαλείας	
	Ενσωμάτωση σε εφεδρικά συστήματα	
	Συστήματα αδιάλειπτης παροχής ισχύος (π. χ. UPS, μπαταρίες, γεννήτριες)	
	Σχέδιο Επιχειρησιακής Συνέχειας (Business Continuity Plan)	
	Σχέδιο αντιμετώπισης εκτάκτου ανάγκης	
	Σχέδιο διαχείρισης συμβάντων και ανάκαμψης από καταστροφές (Disaster Recovery)	
	Επανεξέταση διαδικασιών και συστημάτων	

	εκτάκτου ανάγκης ανά τακτικά χρονικά διαστήματα	
Διαδικασίες για την τακτική δοκιμή, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και των οργανωτικών μέτρων για τη διασφάλιση της ασφάλειας της επεξεργασίας	Διενέργεια vulnerability assessment στα πληροφοριακά συστήματα	
	Διενέργεια penetration tests στα πληροφοριακά συστήματα	
	Εφαρμογή διαδικασίας ελέγχου βασισμένη στην προσέγγιση διαχείρισης κινδύνου, λαμβάνοντας υπόψη με σκοπό την τακτική επανεξέταση, εκτίμηση και αξιολόγηση της αποτελεσματικότητας των τεχνικών και οργανωτικών μέτρων	
Ορισμός Υπευθύνου Προστασίας Δεδομένων	Ορισμός Υπευθύνου Προστασίας Δεδομένων. Εάν έχει οριστεί ΥΠΔ, να σημειωθούν τα στοιχεία επικοινωνίας του	
Μέτρα για την ταυτοποίηση και αδειοδότηση χρηστών - μέτρα για να διασφαλιστεί ότι είναι δυνατή η εκ των υστέρων επαλήθευση και ο προσδιορισμός του εάν και από ποιον έχουν εισαχθεί, τροποποιηθεί ή αφαιρεθεί τα προσωπικά δεδομένα	Αναγνώριση προσωπικού και εξωτερικών συνεργατών που αποκτούν λογαριασμό χρήστη με μοναδικό τρόπο	
	Χρήση ασφαλών Passwords (σύμφωνα με τους εκάστοτε παραδεδεγμένους κανόνες ασφαλείας) με τακτική αυτόματη λήξη και ανανέωση, κλειδώματος μετά από αποτυχημενες προσπάθειες σύνδεσης	
	Διαδικασίες επαλήθευσης εξουσιοδότησης πρόσβασης (Token Authentication/Two-Factor Authentication (2FA)/Multi-Factor Authentication (MFA)/Single Sign on (SSO)	
	Προστασία οθόνης με κωδικό πρόσβασης σε περίπτωση αδράνειας	
	Σύστημα ανίχνευσης εισβολής και σύστημα πρόληψης εισβολής	
	Τακτικά ενημερωμένο πρόγραμμα προστασίας από ιούς	
	Πρόγραμμα προστασίας υποκλοπής (spyware) εγκατεστημένα στο δίκτυο και στους επιμέρους υπολογιστές και τις κινητές συσκευές	
	Πρόσβαση στα δεδομένα προσωπικού χαρακτήρα βάσει περιεχομένου (context-based access)/ χρήστη (user-based access)/ ιδιότητας (role-based access) (διαβαθμισμένη πρόσβαση) κατόπιν αδειοδότησης	
	Σύστημα διαχείρισης χρηστών για τη χαρτογράφηση της βάσης δεδομένων των χρηστών ανάλογα με τις αντίστοιχες εξουσιοδοτήσεις	
Μέτρα για την προστασία των δεδομένων κατά τη διαβίβαση – Απομακρυσμένη Πρόσβαση	Κρυπτογραφημένη μέσω τεχνολογιών TLS/HTTPS ή IPsec	
	VPN με τεχνολογία IPsec ή SSL/TLS	
	Αποτροπή οποιασδήποτε τροποποίησης της διαμόρφωσης VPN του σταθμού διαχείρισης	
Μέτρα για την προστασία των δεδομένων κατά την αποθήκευση	Κρυπτογράφηση κατά την αποθήκευση δεδομένων (encryption at rest) με χρήση hardware keys	
Μέτρα για τη διασφάλιση της φυσικής ασφάλειας των εγκαταστάσεων όπου πραγματοποιείται επεξεργασία δεδομένων προσωπικού χαρακτήρα	Έλεγχος πρόσβασης	
	Έλεγχος εισερχομένων επισκεπτών και συνεργατών	
	Σύστημα ελέγχου πρόσβασης (ανάγνωση κάρτας, κωδικός εισόδου, δαχτυλικό αποτύπωμα κλπ)	
	Σύστημα συναγερμού	

	CCTV Control	
	Προσωπικό Ασφαλείας	
	Μέτρα πυροπροστασίας	
	Συστήματα ελέγχου για την προστασία των συστημάτων από φυσικές ζημιές όπως: ελαττωματικές ηλεκτρικές καλωδιώσεις και συνδέσεις, ανεπαρκή ψύξη και σκόνη, πλημμύρες	
	Σχέδιο ασφάλειας των εγκαταστάσεων	
	Εποπτεία του προσωπικού συντήρησης, τεχνικής υποστήριξης και καθαρισμού από εξουσιοδοτημένο ειδικό	
	Προσήκουσα άδεια πρόσβασης του προσωπικού συντήρησης, τεχνικής υποστήριξης και καθαρισμού	
	Ερμάρια που κλειδώνουν σε περίπτωση επεξεργασίας δεδομένων ειδικής κατηγορίας σε φυσικό αρχείο	
Μέτρα για τη διασφάλιση της καταγραφής περιστατικών ασφάλειας	Λειτουργία καταγραφής συμβάντων (event logs) και συμβάντων ασφαλείας (security incidents) σε όλους τους σταθμούς εργασίας, servers και δικτυακές συσκευές	
	Εφαρμογή συστήματος SOC (Security Operation Center)	
	Χρήση λογισμικού SIEM (Security information and event management	
Μέτρα για τη διασφάλιση της διαμόρφωσης συστημάτων, συμπεριλαμβανομένης της προκαθορισμένης διαμόρφωσης	Πολιτική ασφαλούς διαμόρφωσης εξοπλισμού πληροφορικής και εφαρμογών	
	Πολιτική by design and by default	
Μέτρα για τις εσωτερικές ΤΠ και τη διακυβέρνηση και διαχείριση της ασφάλειας ΤΠ	Πολιτική ΤΠ, διακυβέρνησης και διαχείρισης της ασφάλειας ΤΠ	
Μέτρα για τη διασφάλιση της ελαχιστοποίησης των δεδομένων	Data Minimization pipelines	
Μέτρα για τη διασφάλιση της περιορισμένης διατήρησης των δεδομένων	Πολιτική Διατήρησης & Ασφαλούς Διαγράφης Δεδομένων	
Μέτρα για τη διασφάλιση της λογοδοσίας	Πολιτική αρχείων καταγραφής (Log File Policies)	
Μέτρα που επιτρέπουν τη φορητότητα των δεδομένων και διασφαλίζουν τη διαγραφή τους	Πολιτικές και διαδικασίες για τη χρήση των φορητών μέσων αποθήκευσης (USB, εξωτερικοί σκληροί δίσκοι, CD, DVD), που ανταποκρίνονται στις απαιτήσεις ασφάλειας των συστημάτων και δεδομένων και καλύπτουν τις απαιτήσεις ασφαλούς απομάκρυνσης ή καταστροφής φορητών μέσων	
Μέτρα που αφορούν στο προσωπικό	Ευαισθητοποίηση του προσωπικού και της Διοίκησης σε ζητήματα προσωπικών δεδομένων	
	Εκπαίδευση προσωπικού σε ζητήματα ασφάλειας	
	Περιοδικές υπενθυμίσεις ασφάλειας	
	Εκπαίδευση χρηστών αναφορικά με την προστασία από ιούς	
	Ρήτρα ιδιωτικότητας σε όλες τις συμβάσεις συνεργατών/προσωπικού	
	Διαδικασίες μετά τη λήξη σύμβασης εργασίας (αλλαγή κωδικών πρόσβασης, αφαίρεση/διαγραφή	

	από τον κατάλογο εξουσιοδοτημένων προσώπων, κατάργηση του/των λογαριασμών χρήστη, επιστροφή κλειδιών, καρτών ή άλλων μέσων εισόδου)	
Λοιπά εφαρμοζόμενα μέτρα	Πιστοποίηση ISO27001	
	Πιστοποίηση ISO 9001	
	Πιστοποίηση ISO 27701	
	Πολιτική Προστασίας Προσωπικών Δεδομένων	
	Εκτίμηση Αντικτύπου (DPIA)	
	Πολιτική Διαχείρισης Αιτημάτων Υποκειμένων	

ΠΡΟΣΑΡΤΗΜΑ IV: ΚΑΤΑΛΟΓΟΣ ΥΠΕΡΓΟΛΑΒΩΝ ΕΠΕΞΕΡΓΑΣΙΑΣ

Ο υπεύθυνος επεξεργασίας έχει δώσει άδεια για τη χρήση των παρακάτω υπεργολάβων επεξεργασίας (επωνυμία, στοιχεία επικοινωνίας, παρεχόμενη υπηρεσία, αρμόδιο πρόσωπο):

1. (επωνυμία)

(στοιχεία διεύθυνσης)

(e-mail επικοινωνίας)

(τηλ επικοινωνίας εάν υφίσταται)

(παρεχόμενη υπηρεσία)

(διάστημα επεξεργασίας)

(εφαρμογή κατάλληλων εγγυήσεων σε περίπτωση διαβίβασης δεδομένων εκτός ΕΟΧ)

2.
3.
4.