

Are you ready for GDPR compliance?

Τεχνική & Οικονομική Προσφορά

Αντικείμενο των παρεχόμενων υπηρεσιών

1° Στάδιο

Data Mapping



Το πρώτο στάδιο του έργου συνίσταται στη λεπτομερή αποτύπωση της υπάρχουσας κατάστασης κάθε επιχείρησης, ως προς το νομικό και τεχνολογικό επίπεδο καθώς και ως προς τις πολιτικές και διαδικασίες περί προστασίας προσωπικών δεδομένων. Η αποτύπωση αυτή επιτυγχάνεται μέσω της «χαρτογράφησης» των επεξεργασιών, των ροών δεδομένων και της αποτύπωσης των αλληλεξαρτήσεων.

Στην συγκεκριμένη προσφορά που αφορά το σύνολο των μελών του ΠΟΞ, αναφορικά με το 1° στάδιο η εταιρεία μας προτείνει την σύσταση ομάδας έργου με πρωτοβουλία του ΠΟΞ, η οποία θα αποτελείται από στελέχη, τα οποία θα έχουν γνώση των πολιτικών – διαδικασιών καθώς και των ροών δεδομένων τόσο σε νομικό όσο και πληροφορικό επίπεδο που διέπουν γενικότερα την υφιστάμενη κατάσταση των ξενοδοχείων.



Η ομάδα που θα οριστεί θα βρίσκεται σε συνεχή επικοινωνία με την ομάδα έργου της εταιρείας μας η οποία έχει αποκτήσει μεγάλη εξειδίκευση αφού ήδη έχει συμμορφώσει δεκάδες ξενοδοχεία όλων των κατηγοριών με τον GDPR, ώστε να χαρτογραφηθεί με ακόμα περισσότερη ακρίβεια, η υφιστάμενη κατάσταση των ξενοδοχείων της ΠΟΞ.

Εν συνεχεία τα ευρήματα από την χαρτογράφηση θα ενσωματωθούν σε ερωτηματολόγια, στα οποία θα αποτυπώνεται η συνολική γενική κατάσταση που διέπει τα ξενοδοχεία και θα δοθούν σε κάθε ξενοδοχείο προκειμένου να τα μελετήσουν οι υπεύθυνοι, ώστε αφενός να επιβεβαιώσουν τα κοινά σημεία αφετέρου να υποδείξουν τα σημεία που ενδεχομένως διαφοροποιούνται σε σχέση με την αρχική συνολική αποτύπωση.

Από την επεξεργασία των ερωτηματολογίων που θα μας αποστείλουν τα ξενοδοχεία, θα παραδοθεί στον κάθε υπεύθυνο επεξεργασίας –

ξενοδοχείο η καρτογράφηση της υφιστάμενης κατάστασης για το ξενοδοχείο του. Εφόσον, βάσει των ευρημάτων της αρχικής καρτογράφησης απαιτηθεί και επιτόπιος έλεγχος από την ομάδα έργου μας (αφορά περιπτώσεις με μεγάλες αποκλίσεις) θα υπάρξει επιπλέον επιβάρυνση στα συγκεκριμένα ξενοδοχεία η οποία θα προσδιορίζεται από το εύρος των αποκλίσεων. Ενδεικτικά και όχι περιοριστικά στα πλαίσια του πρώτου σταδίου, αξιολογείται το ακόλουθο υλικό:

- ➔ Η εσωτερική διαδικασία τήρησης των δεδομένων, ήτοι το εσωτερικό επίπεδο ορθής διαχείρισης (συλλογής, καταχώρισης, τήρησης) προσωπικών δεδομένων από το προσωπικό/αρμόδιες διευθύνσεις της επιχείρησης.
- ➔ Τα μέτρα προστασίας του φυσικού και ηλεκτρονικού αρχείου προσωπικών δεδομένων Η σχέση της επιχείρησης με τρίτους (π.χ. πελάτες /προμηθευτές). Οι υπάρχουσες ενημερώσεις προς το προσωπικό ή/και τρίτους αναφορικά με την επεξεργασία δεδομένων. Στο πλαίσιο αυτό διενεργείται έλεγχος των Πολιτικών Απορρήτου & Προστασίας Δεδομένων της επιχείρησης, των εντύπων ενημέρωσης/συγκατάθεσης, των σχετικών όρων σε συμβάσεις εργασίας με το προσωπικό και τους εξωτερικούς συνεργάτες, του υλικού διαδικτυακού μάρκετινγκ κλπ.
- ➔ Τα έντυπα ενημέρωσης/ συγκατάθεσης για την επεξεργασία δεδομένων.
- ➔ Οι υποβληθείσες γνωστοποιήσεις προς την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

2° Στάδιο



Ανάλυση Χάσματος (Gap Analysis) σε σχέση με τις απαιτήσεις του Κανονισμού.

Κατά τη δεύτερη φάση του έργου, αποτυπώνονται τα συμπεράσματα του πρώτου σταδίου, αναφορικά με την υπάρχουσα

κατάσταση ως προς το επίπεδο διαχείρισης και προστασίας δεδομένων και επισημαίνονται τα «κενά» του κάθε ξενοδοχείου ως προς τις προϋποθέσεις συμμόρφωσης που θέτει ο GDPR από νομικής και τεχνολογικής απόψεως.

Παραδοτέο:

- ➔ Θα παραδοθεί σε κάθε ξενοδοχείο υπό τη μορφή εκτενούς και αναλυτικού high level report, η gap analysis στην οποία θα υποδεικνύονται “τα κενά” καθώς και οι απαιτούμενες νομικές και τεχνολογικές ενέργειες για τη «θεραπεία» των ελλείψεων της επιχείρησης από πλευράς προστασίας προσωπικών δεδομένων.

3° Στάδιο

Εκτίμηση Αντικτύπου (Data Privacy Impact Assessment)

Σύμφωνα με το άρθρο 35 του Κανονισμού, όταν ένα είδος επεξεργασίας δεδομένων, ιδίως με τη χρήση νέων τεχνολογιών 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 οφείλει να διενεργεί πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα.



Συνεπώς εφόσον κριθεί από τα συμπεράσματα του gap analysis ότι η επιχείρησή σας φέρει υποχρέωση διεξαγωγής εκτίμησης αντικτύπου για συγκεκριμένες επεξεργασίες της, καθορίζεται η μέθοδος και παραδίδεται στην επιχείρηση η μελέτη εκτίμησης αντικτύπου

Παραδοτέο:

- ➔ Μελέτη στην οποία αποτυπώνονται :
 - ➔ Εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας.

- Εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων.
- Προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων (εγγυήσεις, μέτρα και μηχανισμοί ασφαλείας).

4° Στάδιο

Υλοποίηση & Διασφάλιση Συμμόρφωσης



- Στο τελικό στάδιο της υλοποίησης των προτεινόμενων μέσω του Gap Analysis λύσεων, προκειμένου να επιτευχθεί η συμμόρφωση με τον GDPR, νομικών και τεχνολογικών μέτρων προστασίας προσωπικών δεδομένων, με τις εξής ενέργειες:
- Το σχεδιασμό των Πολιτικών Ασφαλείας και Προστασίας Απορρήτου και Προσωπικών Δεδομένων.
- Την πρόταση των απαραίτητων ενδοεπιχειρησιακών διαδικασιών (“Standard Operating Procedures”) για την ορθή διαχείριση των προσωπικών δεδομένων εντός του Οργανισμού και την «ελαχιστοποίηση» της επεξεργασίας σύμφωνα με τις απαιτήσεις του Κανονισμού.
- Την οργάνωση του «αρχείου επεξεργασιών» του κάθε ξενοδοχείου, ως απαιτείται από τον Κανονισμό, σύμφωνα με την «αρχή της λογοδοσίας», προκειμένου η επιχείρησή σας να είναι σε θέση να αποδεικνύει ανά πάσα στιγμή τη συμμόρφωσή της σε περίπτωση ελέγχου από την Εποπτική Αρχή.
- Τη θέσπιση εσωτερικών διαδικασιών παραλαβής και διεκπεραίωσης αιτημάτων για την ενάσκηση των δικαιωμάτων των υποκειμένων (προετοιμασία κατάλληλων templates για ενημερώσεις των υποκειμένων και για εμπρόθεσμη ικανοποίηση όλων των αιτημάτων τους).
- Τη σύνταξη ή/και τροποποίηση συμβάσεων με εκτελούντες την επεξεργασία.
- Τη σύνταξη/τροποποίηση συμβάσεων με εργαζόμενους, συνεργάτες κλπ.

- Τη θέσπιση/προσαρμογή των απαιτούμενων κατά τον Κανονισμό ενημερώσεων προς το προσωπικό, τους πελάτες, τους διαδικτυακούς χρήστες.
- Την τροποποίηση των εντύπων συγκατάθεσης και τη θέσπιση διαδικασιών εκ νέου λήψης της συγκατάθεσης, ούτως ώστε, στις περιπτώσεις που η συγκατάθεση αποτελεί τη νόμιμη βάση επεξεργασίας των δεδομένων, να πληροί η τελευταία τις απαιτήσεις του Κανονισμού.
- Τη θέσπιση/επικαιροποίηση νομικών εργαλείων διασυννοριακής διαβίβασης δεδομένων.
- Τη θέσπιση διαδικασιών εμπρόθεσμης αναφοράς παραβιάσεων στην Εποπτική Αρχή και στα υποκείμενα των δεδομένων.
- Την εκπαίδευση/επιμόρφωση του προσωπικού αναφορικά με τις νέες υποχρεώσεις τους ως προς την τήρηση και επεξεργασία προσωπικών δεδομένων **(η εκπαίδευση παρέχεται ξεχωριστά, κατόπιν σχετικής συμφωνίας).**



- Τη δυνατότητα παροχής των πληροφοριών του πελάτη, κατόπιν αίτησής του, διασφαλίζοντας την ιδιωτικότητα των δεδομένων
- Τη δυνατότητα τροποποίησης ή πλήρους διαγραφής των στοιχείων του πελάτη από τα συστήματα της επιχείρησης, κατόπιν αίτησής του
- Διάθεση των ευρημάτων που αφορούν τα πληροφοριακά συστήματα στις εταιρείες που σας υποστηρίζουν με λογισμικό και συνεργασία μαζί τους, προκειμένου να

εναρμονισθεί το παρεχόμενο λογισμικό στις απαιτήσεις που ορίζει ο GDPR για την επιχείρησή σας (με επιπλέον χρέωση)

Παραδοτέα:

- ➔ τα νομικά κείμενα που θα διορθωθούν, συμπληρωθούν ή δημιουργηθούν.
- ➔ οι προτάσεις που αφορούν τις ανωτέρω τεχνολογικές λύσεις.

After sales support

(προαιρετικά)

Αφορά στην παροχή εξωτερικών υπηρεσιών Data Protection Officer (εφεξής “DPO”) ή στην εξωτερική συμβουλευτική υποστήριξη του εσωτερικού DPO, κατόπιν συμφωνίας με τον πελάτη.

Ειδικότερα ο ρόλος του DPO:

Σύμφωνα με τα άρθρα 37 επ. του Κανονισμού, κάθε Υπεύθυνος Επεξεργασίας και κάθε Εκτελών την Επεξεργασία *υποχρεούται* να ορίσει DPO εφόσον:

1. είναι δημόσια αρχή/φορέας (εκτός των δικαστηρίων).
2. οι βασικές του δραστηριότητες συνιστούν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα ή
3. οι βασικές του δραστηριότητες συνιστούν μεγάλης κλίμακας επεξεργασία ευαίσθητων δεδομένων (π.χ. δεδομένα υγείας).

Ωστόσο, ακόμα και στις περιπτώσεις όπου ο διορισμός DPO δεν είναι κατά τα ανωτέρω υποχρεωτικός, θα πρέπει να επισημανθεί ότι η ύπαρξη αυτού **συνιστά best practice** για την επιχείρηση στα πλαίσια της αρχής της λογοδοσίας, καθώς, πέραν από την ουσιαστική λειτουργική του χρησιμότητα και συμβολή, καταδεικνύει ότι η επιχείρηση λαμβάνει σοβαρά υπόψη της την προστασία προσωπικών

δεδομένων και τη συμμόρφωση προς το νέο Κανονισμό.

Ο ρόλος του DPO είναι συμβουλευτικός προς τη Διοίκηση και τους υπαλλήλους της επιχείρησης αναφορικά με τις υποχρεώσεις που απορρέουν από τον GDPR και τις λοιπές εθνικές και κοινοτικές διατάξεις περί προστασίας δεδομένων, ενώ έχει επίσης καθήκοντα παρακολούθησης της συμμόρφωσης με το νέο Κανονισμό και με τις Πολιτικές Προστασίας Απορρήτου και Προσωπικών Δεδομένων της επιχείρησης, συμπεριλαμβανομένων και αρμοδιοτήτων ευαισθητοποίησης και κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας των δεδομένων. Επίσης ο DPO θα πρέπει να λειτουργεί ως σημείο επαφής και να συνεργάζεται με την Εποπτική Αρχή για ζητήματα σχετιζόμενα με την επεξεργασία δεδομένων.

Εναπόκειται στη διακριτική ευχέρεια κάθε επιχείρησης να ορίσει είτε εσωτερικό είτε εξωτερικό DPO, θα πρέπει ωστόσο σε κάθε περίπτωση ο DPO να φέρει την κατάλληλη επιστημονική και επαγγελματική εξειδίκευση και να απολαμβάνει τα απαραίτητα εχέγγυα ανεξαρτησίας, υπό την έννοια ότι δεν μπορεί να απολυθεί, ούτε να υποστεί κυρώσεις επειδή επιτέλεσε τα καθήκοντά του. Ο DPO λογοδοτεί απευθείας στο ανώτατο επίπεδο διοίκησης της εταιρείας και θα πρέπει να είναι προσβάσιμος στα υποκείμενα των δεδομένων, για κάθε ζήτημα σχετικό με την επεξεργασία προσωπικών δεδομένων και με την ενάσκηση των δικαιωμάτων τους.

Η TASEIS MANAGEMENT ΕΠΕ παρέχει **outsourced υπηρεσίες DPO**, (εφόσον ο Πελάτης επιθυμεί να ορίσει εξωτερικό DPO), προτείνοντας σας σε κάθε περίπτωση έναν απολύτως εξειδικευμένο επαγγελματία στο πεδίο της προστασίας προσωπικών δεδομένων, ενώ αντίστοιχα αναλαμβάνει την εξωτερική συμβουλευτική υποστήριξη του εσωτερικού DPO της επιχείρησης, σε επίπεδο νομικό και τεχνολογικό, κατόπιν σχετικής συμφωνίας με τον Πελάτη.

Η συμβουλευτική υποστήριξη συνίσταται στη διεξαγωγή τακτικών περιοδικών ελέγχων τήρησης των μέτρων συμμόρφωσης, κατόπιν συμφωνίας με τον πελάτη για την περιοδικότητα αυτών και ενόψει της «επικαιροποίησης» της νομοθεσίας ή και της εισαγωγής νέων διαδικασιών στην επιχείρηση, στην ανταπόκριση σε κάθε ερώτημα της επιχείρησης που αφορά την προστασία προσωπικών δεδομένων, καθώς και στην εκπαίδευση του προσωπικού αναφορικά με τις νέες υποχρεώσεις και δικαιώματα κατά την τήρηση των αρχών προστασίας δεδομένων στην καθημερινή λειτουργία του ξενοδοχείου, στον τρόπο ενημέρωσης των υποκειμένων των δεδομένων (πελατών, εργαζομένων, προμηθευτών κλπ.),

στην αντιμετώπιση των αιτημάτων των υποκειμένων των δεδομένων για την άσκηση των δικαιωμάτων τους, στη διαχείριση περιστατικών παραβίασης δεδομένων κ.ά.

Αναλυτικός Πίνακας Οικονομικής Προσφοράς

Αριθμός Προσωπικού	κόστος
1 ως 5	900 €
6 ως 11	1.200 €
12 ως 17	1.500 €
18 ως 23	1.800 €
24 ως 29	2.100 €
30 ως 40	2.500 €
40 και πάνω	κατόπιν κοινής συνεννόησης

Προκαταβολή: Με την υπογραφή σύμβασης προκαταβάλλεται το 40% της παρούσας προσφοράς.

Α/Α	ΑΝΤΙΚΕΙΜΕΝΟ / ΠΕΡΙΓΡΑΦΗ
1	ΑΠΟΤΥΠΩΣΗ ΥΠΑΡΧΟΥΣΑΣ ΚΑΤΑΣΤΑΣΗΣ («DATA MAPPING»)
2	GAP ANALYSIS Εφόσον κατά την αυτοψία στην ξενοδοχειακή μονάδα προκύψει ανάγκη περαιτέρω ανάλυσης σε επίπεδο: <ul style="list-style-type: none"> • νομικό, • οργανωτικό (πολιτικών και διαδικασιών), • πληροφοριακών συστημάτων της επιχείρησής σας ενδέχεται να υπάρξει επιπλέον οικονομική επιβάρυνση επί της αρχικής προσφοράς όπως αναφέρεται στον πίνακα.
3	ΕΚΤΙΜΗΣΗ ΑΝΤΙΚΤΥΠΙΟΥ (DATA PRIVACY IMPACT ASSESSMENT), εφόσον απαιτείται
4	ΥΛΟΠΟΙΗΣΗ & ΔΙΑΣΦΑΛΙΣΗ ΣΥΜΜΟΡΦΩΣΗΣ
ΕΚΤΙΜΩΜΕΝΟΣ ΧΡΟΝΟΣ ΠΑΡΑΔΟΣΗΣ: 90 ΗΜΕΡΕΣ	

Α/Α	ΑΝΤΙΚΕΙΜΕΝΟ / ΠΕΡΙΓΡΑΦΗ	ΔΙΑΡΚΕΙΑ ΥΠΟΣΤΗΡΙΞΗΣ	ΚΟΣΤΟΣ ΥΠΟΣΤΗΡΙΞΗΣ
1	Υποστήριξη μετά την υλοποίηση του Έργου *after sales support - παροχή συμβουλευτικών υπηρεσιών DPO (προαιρετικά) Η παροχή υπηρεσιών υποστήριξης DPO δύναται να γίνει ανάλογα με τις ανάγκες και τις δυνατότητες της εκάστοτε επιχείρησης ως εξής: <ul style="list-style-type: none"> - παροχή εξωτερικού DPO από τον φορέα μας - συμβουλευτική υποστήριξη του DPO και την ομάδα του (προσωπικό επιχείρησης) - μερική υποστήριξη - ενημέρωση σε σχέση με πιθανές θεσμικές αλλαγές, σε θέματα επικοινωνίας. 	ανά μήνα	Η οικονομική προσφορά θα καθοριστεί μετά την εκτίμηση των απαιτήσεων που θα προκύψουν από την επεξεργασία των ευρημάτων.

Οικονομικοί όροι

- Προκαταβολή 40% με την ανάληψη του έργου και εξόφληση του υπολοίπου 60% τουλάχιστον μια μέρα πριν την ολοκλήρωση του έργου, δηλαδή την παράδοση των σχετικών εγγράφων και των προτάσεων του συμβούλου στην εταιρεία.
- Στο κόστος δεν περιλαμβάνεται ο ΦΠΑ 24%
- Στην προσφορά δεν περιλαμβάνονται τα έξοδα διαμονής, διατροφής και μετακίνησης (εφόσον επρόκειτο για επιχειρήσεις εκτός Αττικής)

