



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ



**εκδδα**

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ  
ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΚΣΤ΄ ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ  
ΤΕΛΙΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ

Προστασία Προσωπικών Δεδομένων και Δικαίωμα  
Ελεύθερης Κυκλοφορίας Προσώπων στον Χώρο  
Σένγκεν

ΤΜ. ΕΞΕΙΔΙΚΕΥΣΗΣ: Γενική Διοίκηση

Επιβλέπων:

Γεώργιος Πατρίκιος

Σπουδάστρια:

Μαρία Κλαουδάτου

ΑΘΗΝΑ – 2020



ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ  
ΥΠΟΥΡΓΕΙΟ ΕΣΩΤΕΡΙΚΩΝ



**εκδδα**

ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ  
ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΚΣΤ΄ ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ  
ΤΕΛΙΚΗ ΕΡΓΑΣΙΑ

ΤΙΤΛΟΣ

Προστασία Προσωπικών Δεδομένων και Δικαίωμα  
Ελεύθερης Κυκλοφορίας Προσώπων στον Χώρο  
Σένγκεν

ΤΜ. ΕΞΕΙΔΙΚΕΥΣΗΣ: Γενική Διοίκηση

Επιβλέπων:

Γεώργιος Πατρίκιος

Σπουδάστρια:

Μαρία Κλαουδάτου

ΑΘΗΝΑ – 2020

ΕΣΔΔΑ, Μαρία Κλαουδάτου Copyright © 2020. Με την επιφύλαξη παντός δικαιώματος.

Δήλωση

«Δηλώνω ρητά ότι, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας, δεν παραβιάζει καθ' οιονδήποτε τρόπο πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής.»

Αθήνα, 20/09/2020

Μαρία Κλαουδάτου.

## Περίληψη

Η υπογραφή της Συμφωνίας Σένγκεν ήταν η αρχή για τη δημιουργία του Χώρου Ελευθερίας, Ασφάλειας και Δικαιοσύνης, προσφέροντας στους πολίτες ελεύθερη μετακίνηση απαλλαγμένη από εσωτερικούς ελέγχους. Ωστόσο αυτό είχε ως αποτέλεσμα την αύξηση των ελέγχων στα εξωτερικά σύνορα, η οποία κυρίως επετεύχθη με την δημιουργία του Συστήματος Πληροφοριών Σένγκεν, ενός συστήματος πληροφοριών μεγάλης κλίμακας, η λειτουργία του οποίου βασίζεται στην συλλογή, αποθήκευση και διαχείριση προσωπικών δεδομένων ατόμων που θα μπορούσαν να απειλήσουν την ασφάλεια του χώρου. Η πρόοδος της τεχνολογίας αλλά και η εξέλιξη του διασυνοριακού οργανωμένου εγκλήματος ωθούσε σε συνεχείς αναβαθμίσεις και τα συστήματα πληροφοριών της Ένωσης. Παράλληλα προέκυψε και η ανάγκη προστασίας θεμελιωδών δικαιωμάτων του ανθρώπου που πιθανόν να πλήττονταν από τη λειτουργία αυτών των συστημάτων, όπως το δικαίωμα στην ιδιωτική ζωή αλλά και το δικαίωμα στην προστασία των προσωπικών δεδομένων. Η ανάγκη αυτή εκφράστηκε με τη θέσπιση ειδικών κανονισμών για την προστασία των δεδομένων αυτών, πέραν των διατάξεων που περιείχονταν ήδη στη νομοθετική βάση του Συστήματος Πληροφοριών Σένγκεν.

Στόχος της παρούσης εργασίας είναι η διερεύνηση της προστασίας των προσωπικών δεδομένων στο Ευρωπαϊκό πλαίσιο του Χώρου Ελευθερίας Ασφαλείας και Δικαιοσύνης σε συνδυασμό με τη λειτουργία των Συστημάτων Πληροφοριών και ιδιαιτέρως του Συστήματος Πληροφοριών Σένγκεν.

Για την πραγμάτευση του θέματος υιοθετείται η μεθοδολογία της παρουσίασης και κριτικής ανάλυσης του σχετικού θεσμικού πλαισίου, της σχετικής νομολογίας του Δικαστηρίου της Ευρωπαϊκής Ένωσης αλλά και γνωμοδοτήσεων και αποφάσεων της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Εισαγωγικά παρουσιάζεται η ιστορική εξέλιξη και λειτουργία της ζώνης Σένγκεν βάσει της συμφωνίας και της σύμβασης εφαρμογής. Παράλληλα παρουσιάζονται οι προσπάθειες προστασίας των προσωπικών δεδομένων των πολιτών στο πλαίσιο αυτών των συνθηκών αλλά και ο πρόσφατος Γενικός Κανονισμός Προστασίας Δεδομένων στις βασικές διατάξεις του. Στη συνέχεια, επιχειρείται παρουσίαση και ανάλυση της νομοθετικής βάσης της λειτουργίας του Συστήματος Πληροφοριών Σένγκεν και του πρόσφατου δεύτερης γενιάς SIS II. Παρουσιάζονται αναλυτικά οι κατηγορίες των δεδομένων που κρατούνται από το σύστημα, ο χρόνος διατήρησης, η πρόσβαση των

αρχών σε αυτά αλλά και τα δικαιώματα του υποκειμένου των δεδομένων. Με την νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης επιχειρείται μία ενδεικτική παρουσίαση της σημασίας της προστασίας των προσωπικών δεδομένων στο Ευρωπαϊκό δίκαιο και της σχέσης τους με το δικαίωμα στην ιδιωτική ζωή ενώ φαίνεται και σημασία της αρχής της αναλογικότητας για την επεξεργασία τους. Η γνωμοδότηση και οι αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επικεντρώνονται στην άσκηση βασικών δικαιωμάτων των υποκειμένων στο πλαίσιο του SIS II. Στο τέλος, επιχειρείται μία συνολική αποτίμηση τόσο του νομοθετικού πλαισίου όσο και της προστασίας των προσωπικών δεδομένων σε αυτό, διαπιστώνονται κίνδυνοι αλλά και μελλοντικές προοπτικές και διατυπώνονται προτάσεις βελτιώσεις ενόψει της θέσπισης νέου νομοθετικού πλαισίου για τα συστήματα πληροφοριών, διαχείρισης συνόρων και επιβολής νόμου στην Ευρωπαϊκή Ένωση.

Η Ευρωπαϊκή Ένωση βρίσκεται σε διαδικασία αναθεώρησης των συστημάτων πληροφοριών, διαχείρισης συνόρων και επιβολής νόμου για να βελτιώσει την αποτελεσματικότητα και την αποδοτικότητα τους. Μάλιστα, τα τελευταία χρόνια η λειτουργία των συστημάτων αυτών φάνηκε να γίνεται αντικείμενο ακόμη πιο έντονου προβληματισμού, καθώς η πρόσφατη προσφυγική κρίση επανέφερε για πρώτη φορά εσωτερικούς ελέγχους και πολιτικές κλειστών συνόρων εντός του Χώρου Ελευθερίας Ασφάλειας και Δικαιοσύνης, κάτι που σήμαινε την ουσιαστική κατάργηση, για ένα διάστημα, της ελεύθερης μετακίνησης που κατοχυρώνονταν από την σύναψη της Συμφωνίας Σένγκεν. Φάνηκε λοιπόν πως η Ευρώπη βιώνει ένα αίσθημα ανασφάλειας που προσπαθεί να θεραπεύσει με μία ισχυρότερη νομοθετική βάση. Παράλληλα όμως τίθεται και το ζήτημα της προστασίας των ανθρωπίνων δικαιωμάτων και των δεδομένων προσωπικού χαρακτήρα που οφείλουν να προστατευτούν ώστε να μην υποχωρήσουν έναντι της ασφάλειας.

Λέξεις – κλειδιά: ελεύθερη μετακίνηση, Σένγκεν, προστασία προσωπικών δεδομένων, διασυνοριακή ροή πληροφοριών, σύστημα πληροφοριών, Ευρώπη

## Summary

The signing of the Schengen Agreement was the beginning of the creation of the Area of Freedom, Security and Justice, offering its citizens free movement without internal border controls. However, this has resulted in increasing external border controls, which was mainly achieved by creating the Schengen Information System, a large-scale information system whose operation is based on the collection and storage of personal data of individuals who could threaten security in the Area. Advances in technology and the evolution of cross-border organized crime have pushed for continuous upgrades in the European Union's information systems. At the same time, the need arose to protect fundamental human rights that may have been affected by the operation of these systems, such as the right to privacy and the right to protection of personal data. This need was expressed through the adoption of specific regulations for the protection of personal data, in addition to the provisions already contained in the legal framework of the Schengen Information System.

The aim of this paper is to investigate the protection of personal data in the European Area of Freedom, Security and Justice in conjunction with the operation of Information Systems and in particular, the Schengen Information System.

For the treatment of the topic, the methodology of the presentation and critical analysis of the relevant institutional framework, the relevant case law of the Court of Justice of the European Union, as well as opinions and decisions of the Personal Data Protection Authority are adopted.

The introduction shows the historical development and operation of the Schengen area under the Schengen agreement and its implementing Convention. At the same time, the efforts of the protection of the personal data of the citizens in this context are presented, as well as the recent General Data Protection Regulation in its basic provisions. Then, a presentation and analysis of the legal basis for the operation of the Schengen Information System and the recent second generation SIS II is attempted. The categories of data held by the system, the retention time, the access of the authorities to them and the rights of the data subject are presented in detail.

The case law of the Court of Justice of the European Union provides an indicative presentation of the importance of the protection of personal data in European law and their relation to the right to privacy, while the principle of proportionality is also important

for their processing. The opinion and decisions of the Personal Data Protection Authority focus on the exercise of fundamental rights of data subjects under SIS II. Finally, a comprehensive assessment of both the legal framework and the protection of personal data is attempted, risks and future prospects are identified and proposals for improvements are made in view of the introduction of a new legal framework for information systems, border management and law enforcement in the European Union.

The European Union is in the process of reviewing information systems, border management and law enforcement to improve their efficiency and effectiveness. In fact, in recent years the operation of these systems has seemed to be of even greater concern, as the recent refugee crisis has reintroduced for the first time internal border controls and closed border policies within the Area of Freedom, Security and Justice, which meant the substantial abolition, for a period of time, of free movement guaranteed by the conclusion of the Schengen Agreement. So, it seems that Europe is experiencing a sense of insecurity that it is trying to cure with a stronger legal basis. At the same time, however, there is the issue of the protection of human rights and personal data that must be protected in order not to compromise on security.

Key words: free movement, Schengen, personal data protection, cross border information flow, information system, Europe

## Πίνακας Περιεχομένων

Περίληψη .....	1
Summary .....	3
Πίνακας Περιεχομένων .....	5
Πίνακας Εικονογράφησης .....	7
Πίνακας Συντμήσεων και Συντομογραφιών .....	8
A. Εισαγωγικά.....	10
A.1. Ιστορική Εξέλιξη Σένγκεν.....	10
A.2 Νομικό Πλαίσιο για την Προστασία Προσωπικών Δεδομένων στην ΕΕ	15
B. Σύστημα πληροφοριών Σένγκεν και Προσωπικά Δεδομένα.....	21
B.1. Σύστημα Πληροφοριών Σένγκεν (SIS) .....	21
B.2. SIS II: Νομοθετική Βάση και Δομή του Συστήματος.....	22
B.3. Διαχειριστική Αρχή eu-LISA .....	23
B.4. Ευρωπαϊός Επόπτης Προστασίας Δεδομένων .....	24
B.5. Η Αρχή της Επικουρικότητας στην ΕΕ μέσα από το SIS II.....	25
B.6. Δεδομένα Προσωπικού Χαρακτήρα στο SIS II.....	26
B.7. Γενικές Παρατηρήσεις .....	35
Γ. Νομολογία και Γνωμοδοτήσεις .....	36
Γ.1. Νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης.....	36
Γ.1.α. Απόφαση C-92/09 και C-93/09 (EU:C:2010:662) .....	36
Γ.1.β Απόφαση C-291-12, EU:C:2013:670 .....	37
Γ.1.γ Η απόφαση C-582/14, EU:C:2016:779.....	38
Γ.1.δ Η απόφαση C-524/06, EU:C:2008:724.....	38
Γ.2. Γνωμοδοτήσεις και Αποφάσεις της Αρχής Δεδομένων Προσωπικού Χαρακτήρα. ....	39
Γ.2.α. Γνωμοδότηση 3/2010 και αποφάσεις που την στηρίζουν.....	39



Γ.2.β Αποφάσεις σχετικά με διαγραφή από SIS λόγω διαγραφής από ΕΚΑΝΑ.....	41
Δ. Τελικά Συμπεράσματα .....	43
Δ.1. Κριτική Θεώρηση της Προστασίας Προσωπικών Δεδομένων στο SIS II .....	43
Δ.2. Προτάσεις – Μελλοντικές Προοπτικές .....	47
Βιβλιογραφία .....	50

## **Πίνακας Εικονογράφησης**

Πίνακας 1: Επιγραμματική παρουσίαση του ΓΚΠΔ 2016/679.....	16
--	----

## Πίνακας Συντμήσεων και Συντομογραφιών

Σύντμηση /Συντομογραφία	Επεξήγηση
<b>ΓΚΠΔ</b>	Γενικός Κανονισμός Προστασίας Δεδομένων
<b>ΔΕΥ</b>	Δικαιοσύνης και Εσωτερικών Υποθέσεων
<b>ΕΕ</b>	Ευρωπαϊκή Ένωση
<b>ΕΕΠΔ</b>	Ευρωπαίος Επόπτης Προσωπικών Δεδομένων
<b>ΕΚΑΝΑ</b>	Εθνικός Κατάλογος Ανεπιθύμητων Αλλοδαπών
<b>ΕΣΔΑ</b>	Ευρωπαϊκή Σύμβαση για τα Δικαιώματα του ανθρώπου
<b>ΚΕΠΠΑ</b>	Κοινή Εξωτερική Πολιτική και Πολιτική Ασφαλείας
<b>ΣΕΕ</b>	Συνθήκη για την Ευρωπαϊκή Ένωση
<b>ΣΕΣΣ</b>	Σύμβαση Εφαρμογής Συμφωνίας Σένγκεν
<b>ΣΛΕΕ</b>	Συνθήκη Λειτουργίας της Ευρωπαϊκής Ένωσης
<b>ΣΠΣ</b>	Σύστημα Πληροφοριών Σένγκεν
<b>ΧΕΑΔ</b>	Χώρος Ελευθερίας, Ασφάλειας και Δικαιοσύνης
<b>CIS</b>	Customs Information System
<b>C.SIS</b>	Central Schengen Information System
<b>C.SIS II</b>	Central Schengen Information System – second generation
<b>DNA</b>	DeoxyriboNucleic Acid
<b>ECRIS</b>	European Criminal Records Information System
<b>ETIAS</b>	European Travel Information and Authorization System
<b>N.SIS</b>	National Schengen Information System
<b>N.SIS II</b>	National Schengen Information System – second generation

<b>SIRENE</b>	Supplementary Information Request at the National Entries
<b>SIS</b>	Schengen Information System
<b>SIS II</b>	Schengen Information System – second generation
<b>VIS</b>	Visa Information System

## A. Εισαγωγικά

Στο παρόν κεφάλαιο της εργασίας παρουσιάζεται η ιστορική εξέλιξη του νομοθετικού πλαισίου της ζώνης Σένγκεν και βασικές έννοιες συστημάτων και οργανισμών που ιδρύθηκαν ως αντιστάθμισμα στο έλλειμα ασφάλειας που θα δημιουργούσε η ουσιαστική κατάργηση των εσωτερικών συνόρων. Στο δεύτερο μέρος γίνεται αναφορά στην προσπάθεια προστασίας των δεδομένων προσωπικού χαρακτήρα στο Ευρωπαϊκό δίκαιο αλλά και μία παρουσίαση των γενικών αρχών που διέπουν τον Γενικό Κανονισμό Προσωπικών Δεδομένων, ο οποίος στοχεύει στην ομοιόμορφη εφαρμογή κανόνων στον τομέα αυτό ανάμεσα στα κράτη μέλη.

### A.1. Ιστορική Εξέλιξη Σένγκεν

Η δημιουργία της Ευρωπαϊκής Ένωσης (ΕΕ), με τη μορφή μιας οντότητας διακριτής από την Ευρωπαϊκή Κοινότητα, συνετελέσθη με την υπογραφή της συνθήκης του Μάαστριχτ στις 7/2/1992. Μάλιστα, ο τρίτος πυλώνας στήριξης της ΕΕ<sup>1</sup> θεμελιώνει την συνεργασία των κρατών μελών στους τομείς της Δικαιοσύνης και των Εσωτερικών Υποθέσεων, ορίζοντας τα θέματα κοινού ενδιαφέροντος για τα κράτη μέλη συμπεριλαμβανομένων κανόνων για την διέλευση προσώπων από τα εξωτερικά σύνορα των κρατών μελών, τους ελέγχους σε αυτά αλλά και τη δικαστική και αστυνομική συνεργασία, τη μεταναστευτική πολιτική και την πολιτική ασύλου (Nugent, 2012). Στην ίδια συνθήκη υιοθετήθηκε και μία από τις σημαντικότερες αρχές της ΕΕ που αφορούσε στην ιθαγένεια της Ένωσης. Βάσει αυτής, κάθε πολίτης κράτους μέλους της Ένωσης είναι ταυτόχρονα και πολίτης της Ένωσης. Αν και η αρχή της ιθαγένειας έχει περισσότερο συμβολικό χαρακτήρα, εκφράζει στην ουσία την ιδέα της ευρωπαϊκής ολοκλήρωσης και από αυτήν απορρέουν δικαιώματα που περιλαμβάνονται στη συνθήκη και απολαμβάνουν οι πολίτες της ΕΕ. Τα δικαιώματα αυτά, πέραν των εκλογικών, αφορούν στην εγκατάσταση και εργασία σε οποιοδήποτε κράτος μέλος της Ένωσης με λίγους περιορισμούς (Nugent, 2012).

Ωστόσο, ακρογωνιαίος λίθος της αρχής της ιθαγένειας δεν μπορούσε παρά να ήταν η ύπαρξη ενός χώρου ελεύθερης μετακίνησης στην Ένωση. Η πορεία προς αυτήν την κατεύθυνση είχε ήδη αρχίσει νωρίτερα, όταν στις 14 Ιουνίου 1985 πέντε κράτη μέλη

---

<sup>1</sup> Η Συνθήκη του Μάαστριχτ χώρισε τις πολιτικές της Ευρωπαϊκής Κοινότητας σε τρεις βασικούς πυλώνες: α) Ευρωπαϊκές Κοινότητες, β) Κοινή Εξωτερική Πολιτική και Πολιτική Ασφαλείας, γ) Αστυνομική και Δικαστική Συνεργασία σε Ποινικές Υποθέσεις. Με την Συνθήκη της Λισαβόνας, οι πυλώνες καταργήθηκαν και απορροφήθηκαν πλήρως από την ΕΕ.

της Ευρωπαϊκής Κοινότητας (Βέλγιο, Γερμανία, Γαλλία, Λουξεμβούργο, Ολλανδία) υπέγραψαν την συμφωνία Σένγκεν, με την οποία καθιερωνόταν η ελεύθερη μετακίνηση προσώπων και εμπορευμάτων για τους υπηκόους αυτών των κρατών αλλά και η δικαστική και αστυνομική συνεργασία. Ουσιαστικός στόχος της συμφωνίας ήταν η κατάργηση των εσωτερικών ελέγχων με την ταυτόχρονη ενίσχυση αυτών στα εξωτερικά σύνορα των κρατών της ζώνης Σένγκεν. Χρειάστηκε, βέβαια, η συμπλήρωση και εξειδίκευση της Συμφωνίας με την υπογραφή της Σύμβασης Εφαρμογής της Συμφωνίας Σένγκεν (ΣΕΣΣ) στις 19 Ιουνίου 1990, ενώ αυτή τέθηκε σε εφαρμογή πέντε χρόνια αργότερα (26 Μαρτίου 1995) δημιουργώντας στην πράξη τη ζώνη Σένγκεν.

Το κεκτημένο Σένγκεν ενσωματώθηκε στο πλαίσιο της ΕΕ μέσω πρωτοκόλλου προσαρτημένου στη συνθήκη του Άμστερνταμ. Παράλληλα, σε ορίζοντα πέντε ετών από την έναρξη ισχύος της συνθήκης, τέθηκε στόχος για εγκαθίδρυση ενός Χώρου Ελευθερίας Ασφαλείας και Δικαιοσύνης (ΧΕΑΔ), προς διευκόλυνση του οποίου, πολιτικές που εντάσσονταν στον έως τότε τρίτο πυλώνα μεταβιβάζονται στην Ευρωπαϊκή Κοινότητα. Ο τρίτος πυλώνας πλέον εξειδικεύεται στην Αστυνομική και Δικαστική Συνεργασία για Ποινικές Υποθέσεις (Nugent, 2012). Η κατάργηση των τριών πυλώνων, καθώς η Ευρωπαϊκή Ένωση αποκτά διεθνή νομική προσωπικότητα με την Συνθήκη της Λισαβόνας, ουσιαστικά μεταφέρει τις εναπομείνασες πολιτικές Δικαιοσύνης και Εσωτερικών Υποθέσεων (ΔΕΥ) στην Συνθήκη Λειτουργίας της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), συγκεντρώνοντάς τις όλες στον τίτλο για τον “Χώρο Ελευθερίας Ασφάλειας και Δικαιοσύνης”. Ένας τέτοιος χώρος περιλαμβάνεται και στους σκοπούς της ΕΕ, όπως αυτοί διατυπώνονται στην Συνθήκη για την Ευρωπαϊκή Ένωση (ΣΕΕ). Δυνάμει λοιπόν αυτής της συνθήκης, το κεκτημένο Σένγκεν εφαρμοζόμενο εντός του θεσμικού και νομικού πλαισίου της ΕΕ, σύμφωνα και με το άρθρο 7 του πρωτοκόλλου Σένγκεν, υπόκειται σε δικαστικό και κοινοβουλευτικό έλεγχο ενώ δεν υπάρχει πλέον δυνατότητα εξαίρεσης για τις νεοεντασσόμενες χώρες μετά τη διεύρυνση του 2004.

Έπειτα από τη σταδιακή ένταξη χωρών στη ζώνη Σένγκεν, σήμερα συμμετέχουν σε αυτήν είκοσι έξι χώρες. Η ένταξη δηλαδή των χωρών στη ζώνη Σένγκεν δεν έχει γίνει εφικτή για όλα τα κράτη μέλη, ενώ κάποιες ιδιομορφίες επιτρέπουν σε τρίτες χώρες να εντάσσονται σε αυτήν με διαφορετικό καθεστώς. Έτσι σύμφωνα με τα στοιχεία της ιστοσελίδας του Ευρωπαϊκού Κοινοβουλίου (Ευρωπαϊκό Κοινοβούλιο, 2020α):

- 21 χώρες είναι κράτη μέλη της ΕΕ (Αυστρία, Βέλγιο, Γαλλία, Γερμανία, Ελλάδα, Εσθονία, Ισπανία, Ιταλία, Ολλανδία, Λετονία, Λιθουανία, Μάλτα,

Λουξεμβούργο, Ουγγαρία, Πολωνία, Πορτογαλία, Σλοβακία, Σλοβενία, Σουηδία, Τσεχία, Φινλανδία)

- 1 χώρα (Δανία) έχει δικαίωμα αυτοεξαίρεσης για κάθε νέο μέτρο στον τομέα ΔΕΥ, Σένγκεν. Πάραυτα δεσμεύεται στο πλαίσιο της κοινής πολιτικής θεωρήσεων.
- 4 χώρες εκτός ΕΕ εντάσσονται υπό το καθεστώς συμμετέχουσας χώρας (Νορβηγία, Ελβετία, Ισλανδία, Λιχτενστάιν)
- 2 χώρες, παρότι μέλη της ΕΕ, εξασφάλισαν ρήτρα εξαίρεσης (Ιρλανδία, Ηνωμένο Βασίλειο)<sup>2</sup>.
- 4 κράτη μέλη ΕΕ (Βουλγαρία, Ρουμανία, Κύπρος, Κροατία) αναμένεται να προσχωρήσουν.

Τα 42.673 χλμ. θαλάσσιων συνόρων και 7.721 χλμ. χερσαίων συνόρων που περιβάλλουν το χώρο Σένγκεν ενέχουν μία αντίθεση. Πιο συγκεκριμένα, για να μπορεί να λειτουργήσει ο προκαθορισμένος χώρος ελευθερίας, όπου η μετακίνηση των προσώπων γίνεται ελεύθερα με απλά έγγραφα ταυτοποίησης και στον οποίο παρέχονται η ασφάλεια, δικαιοσύνη και ελευθερία που αποτελούν στόχους της Ένωσης, απαιτείται περιχαράκωση των εξωτερικών συνόρων. Με άλλα λόγια, καταργούνται επί της ουσίας τα εσωτερικά σύνορα αλλά ενισχύονται τα εξωτερικά, με συνέπεια για κάποιον πολίτη τρίτης χώρας να γίνεται δύσκολο να εισέλθει στη ζώνη Σένγκεν, ωστόσο, εφόσον εισέλθει, κινείται ελεύθερα.

Η κυκλοφορία στον χώρο Σένγκεν συνεπάγεται πλήθος δικαιωμάτων για τους πολίτες των κρατών που συμμετέχουν σε αυτήν από τουρίστες έως εργαζόμενους, φοιτητές και οικογένειες. Με την κατάργηση των εσωτερικών συνόρων, εξασφαλίζεται η ανεμπόδιστη οδική κυκλοφορία, ελαχιστοποίηση των αστυνομικών ελέγχων μόνο για λόγους δημόσιας ασφάλειας ενώ υπάρχουν συγκεκριμένοι όροι και προϋποθέσεις για προσωρινή ή μόνιμη διαμονή, άσκηση επιχειρηματικής δραστηριότητας, σπουδές και έρευνα. Παράλληλα με τα κοινά εξωτερικά σύνορα καθιερώνεται μία ενιαίου τύπου θεώρηση («visa Schengen») για την είσοδο και την κυκλοφορία υπηκόων τρίτων χωρών εντός της ζώνης Σένγκεν.

Όπως είναι φυσικό για να διατηρηθεί το καθεστώς ελευθερίας ήταν απαραίτητο να μην απειληθεί η ασφάλεια και η δικαιοσύνη. Υπήρχε δηλαδή ο φόβος μήπως η

---

<sup>2</sup> Έπειτα από την έξοδο του Ηνωμένου βασιλείου από την ΕΕ, αναμένεται η οριστικοποίηση της συμφωνίας που θα καθορίζει τους όρους μετακίνησης των πολιτών αλλά και την συνεργασία του Ηνωμένου Βασιλείου με την ΕΕ σε θέματα ασφάλειας και Δικαιοσύνης.

κατάργηση των ελέγχων οδηγεί σε αύξηση των παράνομων και εγκληματικών δραστηριοτήτων στο έδαφος των συμβαλλομένων κρατών και για αυτό θεωρήθηκε απαραίτητη η ύπαρξη αντισταθμισμάτων. Κατά συνέπεια από την ΣΕΣΣ προβλέπεται η δημιουργία του Συστήματος Πληροφοριών Σένγκεν (SIS), ενός συστήματος που βοηθά τους συνοριακούς, αστυνομικούς και τελωνειακούς ελέγχους αυτοματοποιώντας τα ερωτήματα και εξυπηρετώντας έτσι αποτελεσματικότερα τη διαδικασία θεωρήσεων (visa). Στην ουσία το SIS βρίσκεται στον πυρήνα της συνεργασίας Σένγκεν και διευκολύνει την αστυνομική και δικαστική συνεργασία αφού παρέχεται αμοιβαία συνδρομή μεταξύ των κρατών στους τομείς της πρόληψης αλλά και αντιμετώπισης του εγκλήματος, έχοντας το δικαίωμα να καταδιώκουν καταζητούμενους στα κράτη του χώρου με την παράλληλη αμοιβαία αναγνώριση των ποινικών υποθέσεων αλλά και την λειτουργία ταχύτερου συστήματος έκδοσης (Ευρωπαϊκό Κοινοβούλιο, 2020β). Πρόκειται δηλαδή για μία κοινή τράπεζα πληροφοριών, στην οποία καταχωρούνται δεδομένα διαθέσιμα για ανταλλαγή μεταξύ των αρμοδίων αρχών. Το SIS διακρίνεται στο κεντρικό σύστημα SIS (C-SIS) και στα εθνικά τμήματα (N-SIS) των συμβαλλομένων κρατών τα οποία συνδέονται με το κεντρικό τμήμα. Ότι δεδομένα εισάγει κάθε εθνικό σύστημα πληροφοριών γίνονται διαθέσιμα και στα υπόλοιπα εθνικά τμήματα μέσω του κεντρικού SIS. Παράλληλα με την ύπαρξη των τμημάτων SIRENE κάθε συμβαλλόμενο μέρος ορίζει ένα όργανο ως σημείο επαφής με τα υπόλοιπα μέρη. Μέσω αυτού διακινούνται όποιες συμπληρωματικές πληροφορίες είναι απαραίτητες.

Οι εξελίξεις των τελευταίων ετών με την αύξηση της τρομοκρατίας, του λαθρεμπορίου, της λαθρομετανάστευσης αλλά κι των αυξημένων προσφυγικών ροών ενέτειναν αυτήν την αίσθηση του ελλείμματος ασφάλειας, καθιστώντας αναγκαία την ανταλλαγή περισσότερων δεδομένων και την βέλτιστη αξιοποίησή τους. Έτσι το SIS αναβαθμίστηκε σε SIS II. Παρόλα αυτά τα συμβαλλόμενα μέλη, εξαρχής της Συμφωνίας Σένγκεν, προχωρούσαν σταδιακά στην εγκαθίδρυση και άλλων συστημάτων ανταλλαγής πληροφοριών και πάγιων φορέων της Ένωσης όπως:

- **Το Σύστημα Europol:** Η Ευρωπαϊκή Αστυνομική Υπηρεσία ιδρύθηκε το 1995 και αποσκοπεί στην αποτελεσματικότερη συνεργασία μεταξύ των αρμοδίων υπηρεσιών των κρατών μελών για την καταπολέμηση του διεθνούς εγκλήματος. Συνδέεται με τα κράτη μέλη μέσω της εθνικής αρμόδιας υπηρεσίας που το καθένα έχει ιδρύσει. Η Europol διατηρεί και διαχειρίζεται ένα ηλεκτρονικό σύστημα πληροφοριών στο οποίο



εισάγονται δεδομένα τόσο από τα κράτη-μέλη όσο και από την ίδια. (Europol, 2020)

- **Το αρχείο της Eurojust:** Με απόφαση του Συμβουλίου την 28η Φεβρουαρίου 2002 συστήνεται η Eurojust, ένα όργανο της ΕΕ στο οποίο κάθε κράτος διορίζει ένα εθνικό μέλος, και του οποίου στόχος είναι η διευκόλυνση της δικαστικής συνεργασίας μεταξύ των κρατών μελών, συντονίζοντας τις έρευνες και τις διώξεις. Βέβαια, για να το κάνει αυτό, δύναται να ανταλλάσσει τις απαραίτητες πληροφορίες με τις εθνικές αρχές μέσω του αυτοματοποιημένου αρχείου δεδομένων που διαθέτει.
- **Το Σύστημα Πληροφοριών για τις Θεωρήσεις (VIS):** Με ένα κεντρικό σύστημα πληροφοριών με το οποίο επικοινωνούν τα κράτη μέλη, διασφαλίζεται η έκδοση ενιαίων θεωρήσεων εισόδου.
- **Το Eurodac:** Ευρωπαϊκό σύστημα για την αντιπαραβολή δακτυλικών αποτυπωμάτων των αιτούντων άσυλο. Ουσιαστικά πρόκειται για μια βάση δεδομένων βιομετρικών στοιχείων, η οποία περιλαμβάνει δακτυλικά αποτυπώματα αιτούντων άσυλο και υπηκόων τρίτων χωρών για αντιπαραβολή και ταυτοποίηση από όλα τα κράτη μέλη. (Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, 2019)
- **Το Σύστημα πληροφοριών των Τελωνείων (CIS):** Ακόμη ένα κοινό αυτοματοποιημένο σύστημα για την διευκόλυνση της τελωνειακής συνεργασίας.
- **Το Ευρωπαϊκό Σύστημα Πληροφοριών Ποινικού Μητρώου (ECRIS):** Πρόκειται για ένα σύστημα το οποίο, μέσα από ένα τυποποιημένο μορφότυπο, διευκολύνει τις ηλεκτρονικές ανταλλαγές πληροφοριών σχετικά με τα ποινικά μητρώα. Η διαφορά με προηγούμενα βρίσκεται στο ότι εδώ δεν πρόκειται για ένα κεντρικό Ευρωπαϊκό σύστημα, αλλά για αποκεντρωμένες βάσεις δεδομένων, οι οποίες συνδέονται μέσω λογισμικού καθιστώντας ευκολότερη και γρηγορότερη την επικοινωνία μεταξύ των κρατών μελών.

## **A.2 Νομικό Πλαίσιο για την Προστασία Προσωπικών Δεδομένων στην ΕΕ**

Γίνεται λοιπόν αντιληπτό από τα παραπάνω πως η ομαλή λειτουργία του ΧΕΑΔ προϋποθέτει αύξηση του επιπέδου ασφαλείας σε αυτόν. Μάλιστα η ραγδαία ανάπτυξη της τεχνολογίας και της πληροφορικής αλλά και οι τρομοκρατικές επιθέσεις από το 2001 και έπειτα έκαναν πιο έντονη αυτή την ανάγκη, καθώς νέες απειλές βρίσκονταν προ των πυλών. Η δημιουργία λοιπόν, συστημάτων πληροφοριών στα οποία θα γινόταν καταχώριση, αποθήκευση, επεξεργασία δεδομένων αλλά και ανταλλαγή αυτών μεταξύ των κρατών μελών, απετέλεσε το βασικό τρόπο διατήρησης της δημόσιας τάξης και ασφάλειας εντός της ζώνης Σένγκεν. Βέβαια, αν και υπήρξε μεγάλη νομοπαραγωγή σχετικά με την κατάρτιση και τη λειτουργία αυτών των συστημάτων, ήταν λιγότερη η νομοθετική δραστηριότητα σε σχέση με την προστασία των δεδομένων που περιέχονται σε αυτά τα συστήματα. Συνεκδοχικά η διαχείριση δεδομένων προσωπικού χαρακτήρα και μάλιστα ενίοτε ειδικών κατηγοριών δεδομένων, η διασφάλιση της νομιμότητας των διαδικασιών αλλά και τα δικαιώματα των υποκειμένων των δεδομένων βρέθηκαν στο προσκήνιο. Βέβαια ο προβληματισμός αυτός δεν ήταν νέος.

Ήδη από το 1950 στο άρθρο 8 της Ευρωπαϊκής Σύμβασης Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ) κατοχυρώνεται το δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής ενώ στη δεκαετία του 1970 θεσπίζονται και οι πρώτοι νόμοι για την προστασία των προσωπικών δεδομένων με τον ΟΟΣΑ το 1980 να εκδίδει «οδηγίες για την προστασία της ιδιωτικότητας και της διασυνοριακής ροής προσωπικών δεδομένων». Ίσως όμως η Σύμβαση 108 για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων, η οποία καταρτίστηκε το 1981 από το Συμβούλιο της Ευρώπης και επικαιροποιήθηκε το 2018 ενσωματώνοντας και τον καινούργιο Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) ήταν το σημαντικότερο βήμα, καθώς παραμένει μέχρι και σήμερα η μοναδική νομικά δεσμευτική διεθνής πράξη στον τομέα αυτό.

Αλλά και στην Ευρωπαϊκή έννομη τάξη το θέμα προσεγγίστηκε με την έκδοση οδηγιών και κανονισμών. Αξίζει βέβαια να σημειωθεί ότι και η ίδια η ΣΕΣΣ περιείχε άρθρα για την προστασία των δεδομένων που υπάρχουν στο σύστημα πληροφοριών Σένγκεν, ενώ αντίστοιχα άρθρα, ειδικά για το SIS, εντοπίζονται στον κανονισμό 1987/2006 του Ευρωπαϊκού Κοινοβουλίου αλλά και στην απόφαση 2007/533/ΔΕΥ του Συμβουλίου της Ευρωπαϊκής Ένωσης. Σε ενωσιακό επίπεδο το δικαίωμα στην προστασία

των προσωπικών δεδομένων κατοχυρώνεται από το 2000 στο άρθρο 8 του Χάρτη Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης, ο οποίος το 2009 με την κύρωση της συνθήκης της Λισαβόνας γίνεται νομικά δεσμευτικός. Η ίδια συνθήκη στο άρθρο 16 αναφέρει ως γενική αρμοδιότητα της ΕΕ να νομοθετεί επί σχετικών ζητημάτων. Ωστόσο είχαν ήδη προηγηθεί δύο οδηγίες που έθεταν την προστασία δεδομένων στην ΕΕ σε υψηλό επίπεδο. Η οδηγία 95/46/ΕΚ (αντικαταστάθηκε από την 2002/58/ΕΚ) μάλιστα, καθιέρωνε και ανεξάρτητες εποπτικές αρχές ενώ η 97/66/ΕΚ ρύθμιζε τα σχετικά ζητήματα στον τομέα των τηλεπικοινωνιών. Τελικά, στις 27 Απριλίου 2016 ψηφίστηκε ο κανονισμός 2016/679 με τίτλο «Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων». Αυτός αντικατέστησε την οδηγία 95/46/ΕΚ και διαμόρφωσε ένα ενιαίο ομοιόμορφο και ισχυρό νομικό πλαίσιο, δεσμευτικό για όλα τα κράτη-μέλη, καθιστώντας ευκολότερη τόσο την οριζόντια εφαρμογή του σε όλα τα κράτη-μέλη όσο και τον έλεγχο. Την ίδια χρονιά ψηφίζεται και η οδηγία 2016/680/ΕΕ που αφορά την επεξεργασία προσωπικών δεδομένων από αρμόδιες αρχές σχετικά με ποινικά αδικήματα ή ποινικές κυρώσεις.

Όπως αναφέρεται στο 1<sup>ο</sup> άρθρο του 2016/680/ΕΕ «Ο παρών κανονισμός θεσπίζει κανόνες που αφορούν την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κανόνες που αφορούν την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα. Παράλληλα στοχεύει στην προστασία θεμελιωδών δικαιωμάτων και στην ομοιόμορφη εφαρμογή του κανονισμού για αυτόν τον σκοπό, δίνοντας παράλληλα το δικαίωμα στα κράτη μέλη να εξειδικεύουν τις διατάξεις του».

Ουσιαστικό πεδίο εφαρμογής του κανονισμού σύμφωνα με το δεύτερο άρθρο του είναι φυσικά πρόσωπα, ανεξαρτήτως ιθαγένειας ή τόπου διαμονής τόσο σχετικά με την αυτοματοποιημένη επεξεργασία προσωπικών δεδομένων τους όσο και την μη αυτοματοποιημένη, εάν αυτά περιέχονται ή πρόκειται να περιληφθούν σε σύστημα αρχειοθέτησης. Ωστόσο ο κανονισμός δεν εφαρμόζεται όταν η επεξεργασία των δεδομένων από τα κράτη μέλη αφορά θέματα Κοινής Εξωτερικής Πολιτικής και Πολιτικής Ασφαλείας (ΚΕΠΠΑ). Επίσης όταν η επεξεργασία γίνεται για ποινικούς λόγους είτε για λόγους δημόσιας ασφάλειας, εφαρμόζεται ως ειδικότερη η Οδηγία 2016/680.

Ο κανονισμός καλύπτει εκτενώς τα θέματα περί επεξεργασίας και τα δικαιώματα του υποκείμενου των δεδομένων όπως σχεδιαγραμματικά φαίνεται στον παρακάτω πίνακα.

Κεφάλαιο 1 (άρθρα 1 - 4)	Γενικές Διατάξεις (αντικείμενο, στόχοι, πεδίο εφαρμογής)
Κεφάλαιο 2 (άρθρα 5 - 11)	Αρχές (αρχές επεξεργασίας, νομιμότητα επεξεργασίας, συγκατάθεση)
Κεφάλαιο 3 (άρθρα 12 - 23)	Δικαιώματα Υποκειμένου
Κεφάλαιο 4 (άρθρα 24 - 43)	Υπεύθυνος και Εκτελών την Επεξεργασία (καθήκοντα, υποχρεώσεις, ασφάλεια)
Κεφάλαιο 5 (άρθρα 44 - 50)	Διαβίβαση σε Τρίτες Χώρες ή Διεθνείς Οργανισμούς
Κεφάλαιο 6 (άρθρα 51 - 59)	Ανεξάρτητες Εποπτικές Αρχές
Κεφάλαιο 7 (άρθρα 60 - 76)	Συνεργασία και Συνεκτικότητα (μεταξύ εποπτικών αρχών, αμοιβαία συνδρομή, Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων)
Κεφάλαιο 8 (άρθρα 77 - 84)	Προσφυγές, Ευθύνες και Κυρώσεις
Κεφάλαια 9-11 (άρθρα 85 - 99)	Ειδικές Περιπτώσεις Επεξεργασίας, Κατ' εξουσιοδότηση Πράξεις και Τελικές Διατάξεις.

*Πίνακας 1: Επιγραμματική παρουσίαση του ΓΚΠΔ 2016/679*

Το άρθρο 5 του ίδιου κανονισμού καθορίζει τις θεμελιώδεις αρχές επεξεργασίας<sup>3</sup> που θα πρέπει να συντρέχουν σωρευτικά για να θεωρείται νόμιμη η επεξεργασία των δεδομένων.

Πρώτη αναφέρεται η **αρχή της νομιμότητας, αντικειμενικότητας και διαφάνειας** περί της σύννομης και θεμιτής επεξεργασίας με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων. Με άλλα λόγια, θα πρέπει να υπάρχει μία βάση που νομιμοποιεί την επεξεργασία, το υποκείμενο να ενημερώνεται για την επεξεργασία με τρόπο ευσύνοπτο, σαφή και εύκολα προσβάσιμο. Η διαφάνεια συνδέεται με αυτόν τον τρόπο και με την **Αρχή της Λογοδοσίας** του υπεύθυνου επεξεργασίας, η οποία τον

<sup>3</sup> Στο άρθρο 4 του ίδιου κανονισμού, ως πράξεις επεξεργασίας ορίζονται «η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή»

καθιστά αποκλειστικά υπεύθυνο για την τήρηση του κανονισμού και την απόδειξη της νομιμότητας της επεξεργασίας. Έτσι σύμφωνα με αυτή, ο υπεύθυνος επεξεργασίας υποχρεούται να επιλέξει την κατάλληλη νομική βάση εκ των προβλεπόμενων στα άρθρα 6 (για τα απλά δεδομένα) και 9 (για τα δεδομένα ειδικών κατηγοριών) του ΓΚΠΔ, να τεκμηριώσει την επιλογή της και να φροντίσει για την ενημέρωση του υποκειμένου των δεδομένων.

Άλλες αρχές είναι αυτή του **περιορισμού του σκοπού** σύμφωνα με την οποία «η συλλογή και επεξεργασία προσωπικών δεδομένων πρέπει να γίνεται για καθορισμένους, ρητούς και νόμιμους σκοπούς και τα δεδομένα να μην υποβάλλονται σε περαιτέρω επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς αυτούς». Η επεξεργασία ωστόσο αυτών για λόγους δημοσίου συμφέροντος εξαιρείται. Επίσης η **αρχή της αναλογικότητας (ελαχιστοποίηση των δεδομένων)** επιβάλλει την συνάφεια, προσφορότητα και αναγκαιότητα των δεδομένων προς τους επιδιωκόμενους σκοπούς επεξεργασίας, ενώ σύμφωνα με την **αρχή της ακρίβειας των δεδομένων** τα δεδομένα θα πρέπει να είναι ακριβή και, όταν είναι αναγκαίο, να επικαιροποιούνται, να διαγράφονται ή να διορθώνονται σε συνάρτηση με τους σκοπούς επεξεργασίας. Παράλληλα η ταυτοποίηση δεδομένων και του υποκειμένου τους θα πρέπει να είναι δυνατή μόνο για το αναγκαίο διάστημα που ορίζουν οι σκοποί της επεξεργασίας (**περιορισμός της περιόδου αποθήκευσης**). Πιθανές εξαιρέσεις υφίστανται, όπως αναφέρει το ίδιο άρθρο «για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον ή σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, εφόσον λαμβάνονται κατάλληλα οργανωτικά μέτρα για τη διασφάλιση των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων». Τέλος η **αρχή της ακεραιότητας και εμπιστευτικότητας** αφορά στην διασφάλιση των δεδομένων, κατά την επεξεργασία τους, από τυχόν παραβίαση, απώλεια, καταστροφή ή φθορά.

Στο άρθρο 6 του ΓΚΠΔ αναλύονται οι προϋποθέσεις της νόμιμης επεξεργασίας των προσωπικών δεδομένων, μία εκ των οποίων πρέπει να ισχύει τουλάχιστον. Έτσι η συναίνεση του υποκειμένου, η συμμετοχή του ως συμβαλλόμενο μέρος κατά τη σύναψη ή την εκτέλεση σύμβασης, η διαφύλαξη του ζωτικού συμφέροντος του ίδιου ή άλλου φυσικού προσώπου, το δημόσιο συμφέρον είναι η άσκηση δημόσιας εξουσίας είναι μερικές από αυτές. Επίσης, η επεξεργασία νομιμοποιείται εάν «είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπεύθυνου επεξεργασίας» ή «για σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος».

Αυτό που παρουσιάζει ενδιαφέρον στο συγκεκριμένο άρθρο του κανονισμού είναι η δυνατότητα που δίνει στα κράτη-μέλη να θεσπίζουν ειδικότερες διατάξεις για την προσαρμογή της εφαρμογής των κανόνων επεξεργασίας, για τη συμμόρφωση με έννομες υποχρεώσεις του υπεύθυνου επεξεργασίας αλλά και για την επεξεργασία για λόγους δημοσίου συμφέροντος. Μάλιστα η βάση για την επεξεργασία μπορεί να ορίζεται σύμφωνα με το δίκαιο της ΕΕ ή το δίκαιο του κράτους-μέλους. Παράλληλα σε σχέση με τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που αναλύονται στο άρθρο 9 φαίνεται να είναι δυνατή η επεξεργασία τους, για λόγους προληπτικής ή επαγγελματικής ιατρικής, για λόγους δημοσίου συμφέροντος και στον τομέα της δημόσιας υγείας, πάντα αναλογικά του επιδιωκόμενου στόχου και με πρόβλεψη για τη διασφάλιση των θεμελιωδών δικαιωμάτων. Αυτό μπορεί να προκαλέσει ανομοιογένεια εφαρμογής των κανόνων μεταξύ των κρατών μελών – κάτι το οποίο στόχευε να θεραπεύσει ο συγκεκριμένος κανονισμός – αλλά ταυτόχρονα διαφαίνεται και μία ασάφεια στην ερμηνεία των εννοιών του δημοσίου συμφέροντος, το οποίο αφήνει περιθώριο διαφορετικών ερμηνειών του σκοπού επεξεργασίας, ακόμη και τροποποίησής του προς συγκεκριμένη κατεύθυνση.

Τέλος, ο 2016/679/ΕΕ στο 3<sup>ο</sup> κεφάλαιο ορίζει τα δικαιώματα του υποκειμένου των δεδομένων. Βασικό δικαίωμα του υποκειμένου είναι αυτό της συνοπτικής, κατανοητής, εύκολα προσβάσιμης και διαφανούς ενημέρωσης, όπως προβλέπεται στο άρθρο 12 του κανονισμού. Το υποκείμενο πρέπει να ενημερώνεται κατά τη συλλογή των δεδομένων για την αναγκαιότητα εκχώρησής τους, τις συνέπειες αυτής καθώς και για οποιαδήποτε πιθανή περαιτέρω επεξεργασία τους. Επίσης, θα πρέπει να γνωρίζει ποιος εκτελεί την επεξεργασία και να μπορεί να άρει τη συγκατάθεση. Ακόμη κατοχυρώνεται το δικαίωμα της πρόσβασης του υποκειμένου στα δεδομένα που το αφορούν, γνωστοποίησης σε αυτό οποιασδήποτε κοινοποίησης των δεδομένων, το χρονικό διάστημα αποθήκευσης τους και πιθανή ύπαρξη αυτοματοποιημένης λήψης αποφάσεων (πχ. κατάρτιση προφίλ). Το υποκείμενο έχει το δικαίωμα να λάβει αντίγραφα των δεδομένων που υποβάλλονται σε επεξεργασία ενώ μπορεί να υποβάλλει και καταγγελία σε εποπτική αρχή. Άλλα δικαιώματα του υποκειμένου είναι η διόρθωση ή διαγραφή (δικαίωμα στη λήθη) αλλά και ο περιορισμός της επεξεργασίας που υφίστανται τα δεδομένα του. Το δικαίωμά της εναντίωσης στην επεξεργασία δεδομένων που αφορούν το υποκείμενο κατοχυρώνεται στο άρθρο 21 ενώ στο 22 της ανθρώπινης παρέμβασης σε απόφαση που λαμβάνεται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας. Χαρακτηριστικό είναι ότι και εδώ η ΕΕ και τα κράτη μέλη δύναται να

διατηρούν ή να θεσπίζουν περιορισμούς κατά τη συλλογή και επεξεργασία των προσωπικών δεδομένων και μάλιστα αρκετά από τα δικαιώματα δύναται να υποχωρήσουν έναντι του δημοσίου συμφέροντος.

Ο ΓΚΠΔ δεν εφαρμόζεται, ωστόσο, στην επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα όργανα και οργανισμούς της ΕΕ. Έτσι θεωρήθηκε απαραίτητο να εκδοθεί και ένας κανονισμός για την προστασία των προσωπικών δεδομένων που να εφαρμόζεται σε όλα τα θεσμικά όργανα και οργανισμούς της ΕΕ ώστε να εξασφαλιστεί ένα ισχυρό και συνεκτικό πλαίσιο προστασίας των δεδομένων στην Ένωση. Η εφαρμογή του θα γινόταν παράλληλα με τον ΓΚΠΔ 2016/679. Πράγματι στις 23/10/2018 εκδόθηκε ο κανονισμός (ΕΕ) 1725/2018 «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ». Η πλειοψηφία των διατάξεων του ταυτίζεται με αυτές του ΓΚΠΔ επιβεβαιώνοντας τον ενιαίο χαρακτήρα τους. Γίνεται λοιπόν κατανοητό πως ο ΓΚΠΔ από μόνος του είναι μόνο μια έκφανση της προστασίας δεδομένων στην ΕΕ και τον χώρο Σένγκεν, αφού συμπληρώνεται με ειδικότερες διατάξεις άλλων κανονισμών, οδηγιών και αποφάσεων.

## **B. Σύστημα πληροφοριών Σένγκεν και Προσωπικά Δεδομένα**

### **B.1. Σύστημα Πληροφοριών Σένγκεν (SIS)**

Η δημιουργία του Συστήματος Πληροφοριών Σένγκεν προβλέπεται ήδη από το άρθρο 92 της ΣΕΣΣ, με έδρα της Υπηρεσίας Τεχνικής Υποστήριξης, όπως η ΣΕΣΣ ονομάζει το κεντρικό SIS (C.SIS), το Στρασβούργο και υποχρέωση κάθε συμβαλλόμενου μέρους για δημιουργία, λειτουργία και συντήρηση μία εθνικής βάσης πληροφοριών (N.SIS), η οποία θα συνδέεται με την κεντρική. Παράλληλα, προβλέπεται και η ύπαρξη των τμημάτων SIRENE για την διακίνηση των επιρόσθετων πληροφοριών.

Το σύστημα SIS βασίστηκε σε αναζήτηση με αυτοματοποιημένα ερωτήματα με σκοπό την προειδοποίηση αστυνομικών και τελωνειακών αρχών σχετικά με επικίνδυνα πρόσωπα ή αντικείμενα που είναι καταχωρημένα στο σύστημα. Τα γραφεία SIRENE αναλαμβάνουν την ανταλλαγή συμπληρωματικών πληροφοριών σε περίπτωση που η αναζήτηση ήταν θετική.

Ήδη από τον τίτλο III της ΣΕΣΣ, προβλέπονται όροι και προϋποθέσεις της αστυνομικής συνεργασίας και της δικαστικής συνδρομής με ακριβή προσδιορισμό των εγκλημάτων για τα οποία αυτή πραγματοποιείται και των προϋποθέσεων υπό τις οποίες επιτρέπεται. Παράλληλα, όσον αφορά τις κατηγορίες δεδομένων που καταχωρούνται στο σύστημα, αυτές αναφέρονται λεπτομερώς στο άρθρο 94. Στο κεφάλαιο 3 του ίδιου τίτλου γίνεται πρόβλεψη για την προστασία των δεδομένων προσωπικού χαρακτήρα και την ασφάλεια αυτών στα πλαίσια του SIS. Γίνεται λοιπόν αναφορά στην καταχώρηση, διατήρηση και έλεγχο των δεδομένων αλλά και στα δικαιώματα του υποκειμένου των δεδομένων. Ταυτόχρονα προβλέπεται η δημιουργία κοινής ελεγκτικής αρχής για το θέμα αυτό αλλά και για τη λειτουργία του συστήματος SIS γενικά. Μάλιστα στον τίτλο IV αναφέρεται η ανάγκη θέσπισης εθνικής νομοθεσίας από καθένα από τα συμβαλλόμενα μέρη σχετικά με την αυτόματη επεξεργασία δεδομένων προσωπικού χαρακτήρα τα οποία μεταβιβάζονται σύμφωνα με την ΣΕΣΣ. Στον ίδιο τίτλο δίνονται γενικές κατευθυντήριες γραμμές όσον αφορά στην επεξεργασία τέτοιων δεδομένων και τη διαβίβασή τους.

Γίνεται λοιπόν κατανοητό ότι ήδη από τις αρχές της εφαρμογής της συμφωνίας Σένγκεν η σύνδεση μεταξύ αύξησης της ασφάλειας και της ελευθερίας ήταν δεδομένο να επηρεάσει θεμελιώδη δικαιώματα και την ιδιωτικότητα του ατόμου. Η συλλογή, διατήρηση και επεξεργασία προσωπικών δεδομένων για τους σκοπούς της εφαρμογής



της ΣΕΣΣ οριοθετείται από τότε ακόμα. Όμως με την προσχώρηση όλο και περισσότερων κρατών μελών στη συμφωνία και ιδιαίτερα μετά την κοινοτικοποίηση του κεκτημένου Σένγκεν, θεωρήθηκε απαραίτητη η αναβάθμιση του συστήματος. Πλέον ο έλεγχος της Συμφωνίας Σένγκεν γίνεται αποτελεσματικότερος αφού υπάρχουν οι κατάλληλες προϋποθέσεις για έλεγχό του, πολιτικό και δικαστικό. Μετά από πολλές συζητήσεις και προσπάθειες θεσπίστηκε το SIS II, δηλαδή το Σύστημα Πληροφοριών Σένγκεν δεύτερης γενιάς, αλλά και το νέο Σύστημα Θεωρήσεων (VIS).

## **B.2. SIS II: Νομοθετική Βάση και Δομή του Συστήματος**

Οι τρομοκρατικές επιθέσεις της 11ης Σεπτεμβρίου 2001 ώθησαν και τις κυβερνήσεις της ΕΕ να λάβουν μέτρα ώστε να ενισχυθεί η καταπολέμηση της τρομοκρατίας. Τα μέτρα αυτά τέθηκαν σε εφαρμογή πριν από την ενσωμάτωσή τους στο SIS II καθώς θεωρήθηκαν άμεσου ενδιαφέροντος. Χαρακτηριστικά αναφέρεται πως ήδη από τη συνεδρίαση του Συμβουλίου Δικαιοσύνης και Εσωτερικών Υποθέσεων της 19/12/2002, δόθηκε στη Europol και τη Eurojust το δικαίωμα πρόσβασης στο SIS. Επίσης στα συμπεράσματα του Συμβουλίου της 5-6/06/2003, συμφωνήθηκε η αποθήκευση και μεταφορά βιομετρικών δεδομένων, κάτι το οποίο αργότερα προστέθηκε στο SIS II.

Τα μέτρα αυτά υιοθετήθηκαν κατά τη δημιουργία του SIS II. Πλέον η νομοθετική του βάση είναι ο κανονισμός (ΕΚ) 1987/2006 «σχετικά με την δημιουργία, τη λειτουργία και τη χρήση του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) «όσον αφορά τα θέματα καταχωρήσεων που ανήκουν στο Πεδίο εφαρμογής του πρώην πρώτου πυλώνα». Παράλληλα η απόφαση του Συμβουλίου Εξωτερικών Υποθέσεων της ΕΕ 2007/533/ΔΕΥ «σχετικά με την εγκατάσταση, λειτουργία και τη χρήση του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II)» αποτελεί τη νομοθετική βάση για τα θέματα που εμπίπτουν στο πεδίο εφαρμογής της ΣΕΕ. Ακόμη υφίσταται και ο κανονισμός του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου 1986/2006 «σχετικά με την πρόσβαση στο Σύστημα Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) των υπηρεσιών των κρατών μελών που είναι υπεύθυνες για την έκδοση αδειών κυκλοφορίας οχημάτων». Όπως αναφέρεται και στο σκεπτικό της απόφασης 2007/533/ΔΕΥ, οι χωριστές πράξεις που απαρτίζουν την νομοθετική βάση δεν επηρεάζουν τον ενιαίο χαρακτήρα της λειτουργίας του SIS II. Για αυτό τόσο στον κανονισμό 1987/2006 όσο και στην απόφαση 533/2007 υπάρχουν πανομοιότυπες διατάξεις.

Η δομή του SIS II όπως περιγράφεται στη νομοθετική του βάση, ακολουθεί εκείνη του SIS I. Έτσι έχουμε το κεντρικό σύστημα (C.SIS II) και τα εθνικά συστήματα τα οποία δημιουργεί κάθε συμβαλλόμενο μέρος (N.SIS II). Η ανταλλαγή των πληροφοριών δεν γίνεται απευθείας μεταξύ των εθνικών συστημάτων αλλά μέσω του κεντρικού συστήματος ενώ κάθε N.SIS II έχει ένα αντίγραφο του αρχείου δεδομένων της βάσης δεδομένων του C.SIS II. Σύμφωνα με το άρθρο 7 της απόφασης 533/2007 το κάθε κράτος μέλος οφείλει να ορίσει μία αρχή που θα έχει κεντρική ευθύνη για το N.SIS II και θα είναι υπεύθυνη για την ομαλή λειτουργία και την ασφάλεια αυτού, εξασφαλίζοντας την πρόσβαση των αρμοδίων αρχών στο SIS II και τη συμμόρφωση με τις διατάξεις της απόφασης. Εκτός από τα εθνικά τμήματα N.SIS II τα κράτη ορίζουν και τις αρχές που θα είναι υπεύθυνες για την ανταλλαγή συμπληρωματικών πληροφοριών (τμήματα SIRENE). Οι συμπληρωματικές πληροφορίες αφορούν οποιαδήποτε πληροφορία δεν είναι αποθηκευμένη στη βάση του SIS II και είναι αναγκαία η ανταλλαγή της για αλληλοενημέρωση μεταξύ των κρατών αλλά και έλεγχο της ποιότητας των δεδομένων ή άσκηση των δικαιωμάτων πρόσβασης σε αυτά. Τα τμήματα αυτά περιλαμβάνονται στον κατάλογο υπηρεσιών N.SIS και τμημάτων SIRENE (2018/C 226/02).

### **B.3. Διαχειριστική Αρχή eu-LISA**

Η διαχειριστική αρχή του SIS II εδρεύει στο Ταλίν της Εσθονίας και είναι ο «Ευρωπαϊκός Οργανισμός για τη Λειτουργική Διαχείριση Συστημάτων ΤΠ Μεγάλης Κλίμακας στον Χώρο Ελευθερίας, Ασφάλειας και Δικαιοσύνης» (eu-LISA). Η λειτουργική διαχείριση αυτών των συστημάτων – ουσιαστικά πρόκειται για τα SIS II, VIS, Eurodac – βοηθά στην υλοποίηση των πολιτικών της ΕΕ στον τομέα ΔΕΥ.

Ο eu-LISA παρέχει τεχνολογική υποστήριξη στα κράτη μέλη και «εξασφαλίζει την ουσιαστική, ασφαλή και συνεχή λειτουργία των συστημάτων τεχνολογίας πληροφοριών. Επίσης είναι υπεύθυνος για την λήψη των αναγκαίων μέτρων για την ασφάλεια των συστημάτων και την ασφάλεια των δεδομένων» (Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, 2019, σελ. 389). Με αυτόν τον τρόπο βοηθά να εξασφαλιστεί η ελεύθερη διακίνηση των Ευρωπαίων εντός της ΕΕ, χωρίς να διακυβεύεται η ασφάλεια της Ευρώπης.

Ταυτόχρονα ασχολείται και με την ανάπτυξη τεχνολογιών που βελτιστοποιούν και κάνουν πιο σύγχρονο και αξιόπιστο το σύστημα διαχείρισης συνόρων της ΕΕ.

«Παρέχει το τεχνικό και λειτουργικό πλαίσιο, ώστε να εξασφαλίζεται ότι οι άνθρωποι που κατοικούν στην ΕΕ μπορούν να ζουν, να εργάζονται και να ταξιδεύουν κατά τρόπο που να ανταποκρίνεται στις προσδοκίες τους. Ο οργανισμός συνεργάζεται στενά με τις χώρες της ΕΕ, τα θεσμικά όργανα της ΕΕ και τους οργανισμούς που δραστηριοποιούνται στον τομέα της δικαιοσύνης και των εσωτερικών υποθέσεων» (Ευρωπαϊκή Ένωση, 2020α).

#### **B.4. Ευρωπαϊός Επόπτης Προστασίας Δεδομένων**

Η εποπτεία του SIS II πραγματοποιείται από τις κατά τόπους εθνικές εποπτικές αρχές και τον Ευρωπαϊό Επόπτη για τα Προσωπικά Δεδομένα (ΕΕΠΔ). Η ανεξάρτητη αυτή εποπτική αρχή θεσμοθετήθηκε με τον κανονισμό (ΕΚ) 45/2001 με στόχο να ελέγχει την επεξεργασία των προσωπικών δεδομένων στα κοινοτικά όργανα και τους οργανισμούς. Παράλληλα κατέχει και συμβουλευτικό ρόλο για σχετικά ζητήματα. Έτσι διασφαλίζεται ότι κάθε επεξεργασία των δεδομένων αυτών από όργανα και οργανισμούς της Ένωσης, είναι σύμφωνη με τα όσα προβλέπονται στη σχετική νομοθεσία του ΓΚΠΔ αλλά και στην αντίστοιχη νομοθετική βάση του SIS II και γίνονται σεβαστά τα δικαιώματα για την προστασία της ιδιωτικής ζωής. Ο ΕΕΠΔ ιδρύθηκε το 2004 και εδρεύει στις Βρυξέλλες (Ευρωπαϊκή Ένωση, 2020).

Αναλυτικότερα, σύμφωνα με την ιστοσελίδα της Ευρωπαϊκής Ένωσης (2020β), ο ΕΕΠΔ εκτός από τον εποπτικό και συμβουλευτικό του ρόλο προς τα όργανα και τους οργανισμούς της ΕΕ, δύναται να διεξάγει έρευνες και να διεκπεραιώνει καταγγελίες. Παράλληλα συνεργάζεται με τις εθνικές αρχές των κρατών-μελών σχετικά με την προστασία των δεδομένων προσωπικού χαρακτήρα αλλά παρακολουθεί και τις νέες τεχνολογίες που επηρεάζουν το συγκεκριμένο θέμα. Για την εκπλήρωση αυτών των ρόλων λειτουργεί με δύο κύρια τμήματα: Το Τμήμα Εποπτείας και Επιβολής, το οποίο αναλαμβάνει την αξιολόγηση της εφαρμογής των κανόνων σχετικά με τα προσωπικά δεδομένα πάντα στο πλαίσιο των οργάνων και των οργανισμών της ΕΕ και το Τμήμα Πολιτικής και Διαβούλευσης, το οποίο δρα συμβουλευτικά προς τους νομοθέτες της ΕΕ σχετικά με τα θέματα της προστασίας δεδομένων προσωπικού χαρακτήρα.

Σύμφωνα με το άρθρο 61 της απόφασης 2007/5 33/ΔΕΥ, ο ΕΕΠΔ ελέγχει και τις δραστηριότητες επεξεργασίας που γίνονται από τη Διαχειριστική Αρχή, ενώ διεξάγει τακτικό έλεγχο ανά τετραετία σύμφωνα με τα διεθνή πρότυπα, διαβιβάζοντας την έκθεση ελέγχου στα ευρωπαϊκά όργανα. Στο άρθρο 62 της ίδιας απόφασης, δίνεται έμφαση στη

συνεργασία του ΕΕΠΔ με τις εθνικές εποπτικές αρχές και μάλιστα ορίζεται πώς συνεδριάζουν δύο φορές το χρόνο για να εξετάσουν πιθανά προβλήματα που απορρέουν από την ερμηνεία της νομικής βάσης και του κανονισμού για τα δεδομένα. Συγκεκριμένα στο άρθρο αναφέρεται «Οι ανωτέρω αρχές, στα πλαίσια των αντίστοιχων αρμοδιοτήτων τους, ανταλλάσσουν σχετικές πληροφορίες, αλληλοβοηθούνται κατά τη διενέργεια κοινών ελέγχων και επιθεωρήσεων, εξετάζουν τυχόν δυσκολίες κατά την ερμηνεία ή την εφαρμογή της παρούσας απόφασης, διερευνούν προβλήματα που μπορεί να τεθούν κατά την άσκηση ανεξάρτητου ελέγχου ή κατά την άσκηση του δικαιώματος πρόσβασης ενός προσώπου στα δεδομένα που το αφορούν, συντάσσουν ομοιόμορφες προτάσεις ώστε να εξευρεθούν κοινές λύσεις σε τυχόν προβλήματα και προάγουν κατά τον δέοντα τρόπο την ευαισθητοποίηση όσον αφορά τα δικαιώματα για την προστασία των δεδομένων.».

Έτσι σε περίπτωση που κάποιος πολίτης θεωρεί πως έχουν παραβιαστεί βασικά τους δικαιώματα και εφόσον έχει ασκήσει τα δικαιώματα του εναντίον του οργάνου ή του οργανισμού της ΕΕ, το οποίο θεωρεί ότι έκανε την παραβίαση, μπορεί στη συνέχεια να απευθυνθεί στον Υπεύθυνο Προστασίας Δεδομένων και, εφόσον δεν ικανοποιηθεί από τις απαντήσεις, έχει το δικαίωμα να υποβάλλει καταγγελία στον ΕΕΠΔ για διερεύνηση της υπόθεσης. Κατοχυρώνονται λοιπόν με αυτό τον τρόπο δύο από τα βασικά δικαιώματα του υποκειμένου των δεδομένων, σύμφωνα με τον ΓΚΠΔ, αυτό της εναντίωσης και της ενημέρωσης.

## **B.5. Η Αρχή της Επικουρικότητας στην ΕΕ μέσα από το SIS II**

Στο άρθρο 5 της ΣΕΕ κατοχυρώνεται η αρχή της επικουρικότητας, η οποία διέπει τη δράση της ΕΕ κατά την άσκηση των αρμοδιοτήτων της. Έτσι στους τομείς μη αποκλειστικής αρμοδιότητας της ΕΕ, τα κράτη-μέλη δύνανται να αποφασίζουν και λαμβάνουν τα μέτρα που τα ίδια θεωρούν αναγκαία. Η συγκεκριμένη αρχή συμπληρώνει την αρχή της εγγύτητας που αναφέρεται στο 10<sup>ο</sup> άρθρο της ίδιας συνθήκης, κατά την οποία στόχος είναι η άσκηση των αρμοδιοτήτων σε επίπεδο εγγύτερο στους πολίτες. Με άλλα λόγια η αρχή της επικουρικότητας «ορίζει τις προϋποθέσεις υπό τις οποίες η Ένωση έχει προτεραιότητα δράσης έναντι των κρατών μελών στους τομείς που δεν υπάγονται στην αποκλειστική αρμοδιότητά της» (Ευρωπαϊκό Κοινοβούλιο, 2020β)

Η κοινοτικοποίηση του κερτημένου Σένγκεν και μάλιστα η ένταξη του θεσμικού πλαισίου με την Συνθήκη της Λισαβόνας στην ΣΕΕ και ΣΛΕΕ, οδήγησε ουσιαστικά στο πέρασμα από την διακυβερνητική συνεργασία στην μεταβίβαση αρμοδιοτήτων σε

υπερεθνικό επίπεδο. Ήταν λοιπόν λογικό επακόλουθο πως το ενωσιακό επίπεδο ήταν το προσφορότερο για την λήψη μέτρων και αποφάσεων που θα διασφάλιζαν την επιτυχία του ΧΕΑΔ. Εξάλλου η προσχώρηση σε αυτόν τον χώρο των περισσότερων πλέον κρατών-μελών της ΕΕ και όχι μόνο, έκανε επιτακτική την ανάγκη ομοιομορφίας στο νομικό πλαίσιο του SIS κάτι που μόνο κοινή ευρωπαϊκή νομοθεσία θα μπορούσε να επιτύχει. Έτσι τόσο η νομοθετική βάση του SIS II που προαναφέρθηκε όσο και η θέσπιση του ΓΚΠΔ έδωσε στα κράτη μέλη κοινό έδαφος για την αποτελεσματικότερη συνεργασία τους. Μάλιστα η ΕΕ είναι αυτή που χρηματοδοτεί το C.SIS αλλά και τη διαχειριστική αρχή eu-LISA. Χαρακτηριστικά αναφέρεται στο σκεπτικό του κανονισμού 1986/2006 «Δεδομένου ότι **ο σκοπός των μέτρων που πρέπει να ληφθούν**, δηλαδή η παροχή πρόσβασης στο SIS II των υπηρεσιών των κρατών μελών που είναι αρμόδιες για την έκδοση αδειών κυκλοφορίας οχημάτων, ώστε να διευκολύνεται η εκτέλεση των καθηκόντων τους βάσει της οδηγίας 1999/37/EK, **δεν μπορεί να επιτευχθεί επαρκώς από τα κράτη μέλη** και συνεπώς, λόγω της ίδιας της φύσης του SIS II ως κοινού συστήματος πληροφόρησης, **μπορεί να επιτευχθεί μόνο σε κοινοτικό επίπεδο**, η Κοινότητα μπορεί να λάβει μέτρα, **σύμφωνα με την αρχή της επικουρικότητας** όπως ορίζεται στο άρθρο 5 της Συνθήκης.»

Βέβαια, η αρχή της επικουρικότητας φαίνεται από το γεγονός ότι τα κράτη μέλη διατηρούν το δικαίωμα να ορίζουν – και την υποχρέωση να χρηματοδοτούν – τα ίδια τις αρμόδιες αρχές N.SIS και SIRENE, οι οποίες καταχωρίζουν και επεξεργάζονται δεδομένα στις βάσεις δεδομένων ενώ είναι και εγγύτερα στον πολίτη για την άσκηση των δικαιωμάτων του ως υποκείμενο των δεδομένων. Παράλληλα ακόμη και μετά την έκδοση των σχετικών κανονισμών και αποφάσεων δίνεται, σε συγκεκριμένες περιπτώσεις, στα κράτη-μέλη η δυνατότητα να ακολουθήσουν το εθνικό τους δίκαιο ή να θεσπίσουν περαιτέρω διατάξεις εφαρμογής των κανονισμών.

## **B.6. Δεδομένα Προσωπικού Χαρακτήρα στο SIS II**

Όπως προαναφέρθηκε η ελεύθερη μετακίνηση πολιτών στην ζώνη Σένγκεν προϋποθέτει την διασφάλιση της ασφάλειας και της δικαιοσύνης εντός του χώρου. Αναγκαία προϋπόθεση για αυτό είναι η ενίσχυση των εξωτερικών συνόρων. Βέβαια οι νέες μορφές οργανωμένου εγκλήματος αλλά και οι τρομοκρατικές επιθέσεις των τελευταίων ετών έκαναν πιο επιτακτική αυτήν την ανάγκη, η ικανοποίηση της οποίας θεραπεύεται με δημιουργία περισσότερων βάσεων δεδομένων και συστημάτων

πληροφόρησης (SIS II, VIS, Eurodac, CIS). Αυτό συνεπάγεται αύξηση των δεδομένων που συλλέγονται για επεξεργασία και επέκταση της συλλογής και σε ειδικών κατηγοριών προσωπικά δεδομένα, όπως βιομετρικά δεδομένα, γεγονός το οποίο ενέχει κινδύνους για τα ανθρώπινα δικαιώματα και χρειάζεται εξαιρετικά προσεκτική αντιμετώπιση. Αυτός είναι και ο λόγος που οι ίδιοι οι κανονισμοί και οι αποφάσεις περιέχουν λεπτομερείς διατάξεις για την προστασία τους και τα δικαιώματα του υποκειμένου των δεδομένων.

Αναλυτικότερα μελετώντας την νομική βάση του SIS II διαπιστώνεται αρχικά, με τα άρθρα 10,11,16 και 17 της αποφασής 2007/533/ΔΕΥ, η μέριμνα για την ασφάλεια και την εμπιστευτικότητα των δεδομένων που καταχωρίζονται στο SIS II. Τόσο η διαχειριστική αρχή όσο και οι εθνικές αρχές φροντίζουν για αυτήν την διασφάλιση, ο καθένας στο πεδίο των αρμοδιοτήτων του, εκπονώντας σχέδια ασφαλείας για το κεντρικό C.SIS II και για τα N.SIS II αντίστοιχα. Συγκεκριμένα πρέπει να φροντίζουν για τη φυσική προστασία των δεδομένων και να εκπονούν σχέδια έκτακτης ανάγκης για την προστασία των κρίσιμων υποδομών. Παράλληλα οφείλουν να μεριμνούν για μία σειρά ελέγχων όπως αναφέρονται παρακάτω:

- α. Έλεγχος εισόδου εγκαταστάσεων ώστε να μην εισέρχονται σε αυτές μη εξουσιοδοτημένα πρόσωπα.
- β. Έλεγχος των μέσω αποθήκευσης δεδομένων ώστε να μην είναι εφικτή η αλλοίωση ή τροποποίηση τους ή ακόμη και η μεταφορά τους.
- γ. Έλεγχος της καταχώρισης σε αρχείο ώστε να καταχωρίζουν, επεξεργάζονται και διαγράφουν δεδομένα μόνο εξουσιοδοτημένες αρχές και πρόσωπα.
- δ. Έλεγχος της χρήσης ώστε να μη γίνει χρήση των συστημάτων από μη εξουσιοδοτημένα πρόσωπα.
- ε. Έλεγχος των χαρακτηριστικών του προσωπικού και της πρόσβασης σε δεδομένα, ώστε να εξασφαλίζεται με ακρίβεια η καταγραφή των καθηκόντων των αρμοδιοτήτων και των δραστηριοτήτων όλων, όσοι έχουν δικαίωμα πρόσβασης στα δεδομένα του SIS II. Παράλληλα ότι η πρόσβαση χρησιμοποιείται μόνο για τα καθήκοντά τους και αποκλειστικά από τους ίδιους.
- στ. Έλεγχος της διαβίβασης ώστε εξακριβώνεται πού μπορούν να διαβιβάζονται τα δεδομένα.
- ζ. Έλεγχος της εισαγωγής ώστε να εξακριβώνεται η ποιότητα των δεδομένων προσωπικού χαρακτήρα που εισήχθησαν στο σύστημα, ποιος τα εισήγαγε και για ποιο σκοπό.

- η. Έλεγχος της μεταφοράς ώστε με τη μέθοδο της κρυπτογράφησης να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση στα δεδομένα
- θ. Αυτοέλεγχος ώστε μέσω των εσωτερικών ελέγχων να εξακριβώνεται η αποτελεσματικότητα των μέτρων ασφαλείας.

Παράλληλα για να εξασφαλιστεί η εμπιστευτικότητα, εφαρμόζεται ο κανόνας του επαγγελματικού απορρήτου η ισοδύναμου ανάλογα την εθνική νομοθεσία το οποίο επεκτείνεται ακόμη και την παύση των καθηκόντων όλων, όσοι ασχολούνται με τα προσωπικά δεδομένα στο SIS II.

Σε σχέση με την διαχείριση αλλά και την προστασία των προσωπικών δεδομένων η απόφαση 2007/533/ΔΕΥ παρέχει όλο το πλαίσιο για την καταχώριση, τη χρήση και την προστασία των προσωπικών δεδομένων στο SIS II σχετικά με το είδος των δεδομένων που καταχωρούνται, τους σκοπούς της καταχώρισης, το χρόνο διατήρησης, τα δικαιώματα πρόσβασης και επεξεργασίας αλλά και τα δικαιώματα του υποκειμένου. Ειδικότερα:

- ***Σκοποί Επεξεργασίας***

Στο άρθρο 26 της απόφασης 2007/5 33/ΔΕΥ, η καταχώριση, επεξεργασία και διατήρηση των δεδομένων κρίνεται απαραίτητη για πρόσωπα που ζητούνται για σύλληψη και παράδοση η έκδοση κατόπιν ευρωπαϊκού εντάλματος σύλληψης η αιτήματος της δικαστικής αρχής του καταχωρούντος κράτους μέλους. Στο άρθρο 32 της ίδιας απόφασης αναφέρεται στην περίπτωση των εξαφανισθέντων προσώπων τα οποία αναζητούνται είτε για δική τους προστασία είτε για αποτροπή απειλών αλλά και για πρόσωπα που δεν χρήζουν προστασίας. Επίσης είναι δυνατή η αναζήτηση προσώπων με σκοπό τη συμμετοχή στη δικαστική διαδικασία. Έτσι στο άρθρο 34 αναφέρεται πως καταχωρίσεις γίνονται για μάρτυρες σε δικαστική διαδικασία, πρόσωπα που διώκονται και καλούνται να εμφανιστούν ενώπιον δικαστηρίου ή πρόσωπα για τα οποία έχει εκδοθεί καταδικαστική απόφαση η οποία πρέπει να τους επιδοθεί αλλά και πρόσωπα που πρέπει να εμφανιστούν για να εκτίσουν ποινή στερητική της ελευθερίας.

Παράλληλα με το άρθρο 36 επιτρέπεται η εισαγωγή καταχωρήσεων προσώπων και αντικειμένων με σκοπό τη διακριτική παρακολούθηση ή τον ειδικό έλεγχο, πάντα σε συμφωνία με το εθνικό δίκαιο του κράτους-μέλους. Τέτοιες καταχωρήσεις γίνονται μόνο εφόσον υπάρχουν σαφείς ενδείξεις για διάπραξη αξιόποινης πράξης ή εκτίμηση για πιθανή μελλοντική διάπραξη αξιόποινων πράξεων από κάποιο άτομο, βάσει τέλεσης ανάλογων πράξεων στο παρελθόν. Κι εδώ η καταχώριση επιτρέπεται σε περίπτωση

ύπαρξης ενδείξεων σοβαρής απειλής για τη δημόσια τάξη και ασφάλεια. Τέλος το άρθρο 38 θέτει τις προϋποθέσεις εισαγωγής καταχωρήσεων για αντικείμενα που είτε θα χρησιμεύσουν ως αποδεικτικά στοιχεία σε ποινική διαδικασία είτε πρέπει να κατασχεθούν. Συγκεκριμένα καταχωρίζονται:

α) οχήματα κυλινδρισμού κινητήρα άνω των 50 κυβικών εκατοστών, πλοία και αεροσκάφη·

β) ρυμούλκες βάρους, χωρίς φορτίο, άνω των 750 χιλιογράμμων, τροχόσπιτα, βιομηχανικός εξοπλισμός, εξωλέμβιες μηχανές και εμπορευματοκιβώτια·

γ) πυροβόλα όπλα·

δ) ασυμπλήρωτα επίσημα έγγραφα που έχουν κλαπεί, υπεξαιρεθεί ή απολεσθεί·

ε) εκδοθέντα έγγραφα ταυτότητας, όπως διαβατήρια, δελτία ταυτότητας, άδειες οδήγησης, τίτλοι παραμονής και ταξιδιωτικά έγγραφα που έχουν κλαπεί, υπεξαιρεθεί, απολεσθεί ή ακυρωθεί

στ) άδειες κυκλοφορίας οχημάτων και πινακίδες αριθμού κυκλοφορίας που έχουν κλαπεί, υπεξαιρεθεί, απολεσθεί ή ακυρωθεί·

ζ) τραπεζογραμμάτια (προσημειωμένα χαρτονομίσματα)·

η) χρεόγραφα και μέσα πληρωμής, όπως επιταγές, πιστωτικές κάρτες, ομολογίες και μετοχές που έχουν κλαπεί, υπεξαιρεθεί, απολεσθεί ή ακυρωθεί.»

▪ ***Κατηγορίες δεδομένων που καταχωρίζονται***

Το άρθρο 20 της απόφασης 2007/533/ΔΕΥ αναφέρεται στις κατηγορίες δεδομένων που καταχωρίζονται και αποθηκεύονται στο SIS II σύμφωνα με τους σκοπούς που προαναφέρθηκαν. Αποθηκεύονται λοιπόν δεδομένα για πρόσωπα για τα οποία έχει γίνει καταχώριση στο σύστημα αλλά και για αντικείμενα που έχουν καταχωρηθεί σε αυτό. Συγκεκριμένα:

α) επώνυμο ή επώνυμα και όνομα ή ονόματα, το ονοματεπώνυμο του προσώπου κατά τη γέννηση, τυχόν ονοματεπώνυμα που έχουν χρησιμοποιηθεί κατά το παρελθόν και τυχόν ψευδώνυμα, τα οποία μπορούν να εισάγονται χωριστά·

β) τυχόν ιδιαίτερα, αντικειμενικά και αναλλοίωτα φυσικά χαρακτηριστικά·

γ) ημερομηνία και τόπος γέννησης·

δ) φύλο·

ε) φωτογραφίες·

στ) δακτυλικά αποτυπώματα·

ζ) ιθαγένεια ή ιθαγένειες·



- η) ένδειξη ότι το πρόσωπο οπλοφορεί, είναι βίαιο ή έχει αποδράσει·
- θ) λόγος της καταχώρισεως·
- ι) αρχή που εισάγει την καταχώριση·
- ια) μνεία της απόφασης βάσει της οποίας εισάγεται η καταχώριση·
- ιβ) ακολουθητέα τακτική·
- ιγ) σύνδεσμος ή σύνδεσμοι με άλλες καταχωρίσεις που έχουν εισαχθεί στο SIS II δυνάμει του άρθρου 52·
- ιδ) είδος του αδικήματος»

Φυσικά πριν εισάγουν μία καταχώριση τα κράτη-μέλη εκτιμούν την αναλογικότητα των δεδομένων που καταχωρούνται προς το σκοπό της καταχώρισης. Στο άρθρο 22 διευκρινίζεται πως η χρήση φωτογραφιών και δακτυλικών αποτυπωμάτων, γίνεται μόνο κατόπιν ελέγχου ποιότητας των δεδομένων αλλά και χρησιμοποιούνται τα συγκεκριμένα δεδομένα μόνο για επαλήθευση ταυτότητας προσώπου. Η χρήση των δακτυλικών αποτυπωμάτων δεν είναι ακόμα εφικτή λόγω της μη διαθεσιμότητας κατάλληλης τεχνολογίας και γνώμης του Ευρωπαϊκού Κοινοβουλίου.

Εκτός από τα ως άνω δεδομένα, σύμφωνα με το άρθρο 27, στην περίπτωση προσώπων που αναζητούνται για σύλληψη και παράδοση εισάγεται στο σύστημα και αντίγραφο του ευρωπαϊκού εντάλματος σύλληψης. Τέλος στο άρθρο 56 αναφέρεται πως απαγορεύεται ρητά η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων βάσει του άρθρου 6 της σύμβασης του Συμβουλίου της Ευρώπης της 28ης Ιανουαρίου 1981, στο πλαίσιο της προστασίας του ατόμου από την αυτοματοποιημένη επεξεργασία. Η απαγόρευση αυτή είναι κάτι που προβλέπεται και στο άρθρο 9 του ΓΚΠΔ.

#### ▪ *Χρόνος διατήρησης*

Τα σχετικά με το χρόνο τήρησης των δεδομένων εντοπίζονται στο άρθρο 44 της απόφασης 2007/5 33/ΔΕΥ για δεδομένα φυσικών προσώπων και στο άρθρο 45 για δεδομένα αντικειμένων. Σύμφωνα με αυτά, είναι σημαντικό οι καταχωρίσεις που εισάγονται στο σύστημα να διατηρούνται μόνο για το χρονικό διάστημα που θεωρείται απαραίτητο για την επίτευξη του σκοπού εισαγωγή στους (αρχή της αναλογικότητας). Σε κάθε περίπτωση, εντός τριετίας από την εισαγωγή δεδομένων για πρόσωπα το κράτος μέλος που καταχώρισε τα δεδομένα όφειλε να επανεξετάσει τη σκοπιμότητα διατήρησής τους. Μάλιστα εάν πρόκειται για δεδομένα που αφορούσαν σε διακριτική παρακολούθηση η διεξαγωγή ειδικών ελέγχων το διάστημα αυτό είναι ένα έτος. Δύναται κάθε κράτος-μέλος να επανεξετάσει το χρόνο διατήρησης των δεδομένων και σε

μικρότερη χρονική περίοδο πάντα αναλόγως του εθνικού του δικαίου. Εάν το κράτος μέλος αποφασίσει πώς η καταχώριση πρέπει να διατηρηθεί για τους σκοπούς τους οποίους έγινε οφείλει να ενημερώσει το C.SIS II. Σε αντίθετη περίπτωση πρέπει να προχωρήσει στη διαγραφή της καταχώρισης και των δεδομένων. Εάν το κράτος μέλος δεν προβεί σε καμία τέτοια ενέργεια η διαγραφή γίνεται αυτόματα από το κεντρικό σύστημα, το οποίο βέβαια ειδοποιεί το καταχωρούν κράτος τέσσερις μήνες πριν την εκτέλεσή της.

Σχετικά με τη διατήρηση των καταχωρίσεων για τα αντικείμενα, ισχύει και εδώ η αρχή της αναλογικότητας. Το ανώτατο όριο διατήρησης για αντικείμενα που εισάγονται σύμφωνα με το άρθρο 36, περί διακριτικής παρακολούθησης και διεξαγωγής ειδικών ελέγχων, είναι 5 έτη ενώ για καταχωρίσεις που εισάγονται σύμφωνα με το άρθρο 38, περί κατασχέσεων αντικειμένων ή χρησιμοποίησή τους ως αποδεικτικά στοιχεία σε δικαστική διαδικασία, το ανώτατο όριο διατήρησης των δεδομένων είναι 10 έτη. Κι εδώ υπάρχει δυνατότητα παράτασης της διατήρησης εάν αυτό κριθεί απαραίτητο προς τους σκοπούς της καταχώρισης.

Στο άρθρο 53 προσδιορίζεται και ο χρόνος διατήρησης των συμπληρωματικών πληροφοριών που ανταλλάσσονται από τα τμήματα SIRENE. Τα δεδομένα που ήταν απαραίτητη η καταχώρισή τους, φυλάσσονται μόνο για το απαιτούμενο χρονικό διάστημα για την επίτευξη του σκοπού της καταχώρισής τους. Διαγράφονται όμως υποχρεωτικά με την πάροδο ενός έτους από τη διαγραφή της σχετικής καταχώρισης από το SIS II. Παρόλα αυτά τα κράτη μέλη δύνανται να διατηρήσουν στα αρχεία τους για χρονικό διάστημα που ορίζει η εθνική τους νομοθεσία, δεδομένα για τα οποία τα ίδια τα κράτη είχαν εισάγει καταχώριση στο SIS II ή δεδομένα καταχώρισης για την οποία είχαν αναλάβει δράση στο έδαφός τους.

Σε αυτό το σημείο αξίζει να σημειωθεί πώς οι διατάξεις ορίζουν βέβαια συγκεκριμένα χρονικά πλαίσια για τη διαγραφή των καταχωρήσεων, ωστόσο όπως φάνηκε από τις διατάξεις που προαναφέρθηκαν υπάρχει διακριτική ευχέρεια ώστε τα κράτη-μέλη να επανεξετάσουν τη σκοπιμότητα της διατήρησης των δεδομένων και αυτό ίσως είναι μία πηγή ανομοιογενούς εφαρμογής.

#### ▪ *Πρόσβαση στα Δεδομένα*

Το κεφάλαιο 10 της απόφασης 2007/5 33/ΔΕΥ προσδιορίζει τις αρχές που έχουν δικαίωμα πρόσβασης στις καταχωρίσεις. Φυσικά και εδώ ισχύει η αρχή της αναλογικότητας και της ελαχιστοποίησης των δεδομένων αφού οι αρχές που έχουν

δικαίωμα πρόσβασης, λαμβάνουν εκείνα τα δεδομένα που είναι απαραίτητα για το σκοπό τους. Έτσι στο άρθρο 40 προβλέπεται πως πρόσβαση είτε απευθείας στα δεδομένα είτε στο αντίγραφο δεδομένων του SIS II έχουν αρχές αρμόδιες για συνοριακούς, τελωνειακούς και αστυνομικούς ελέγχους και τον συντονισμό αυτών από εντεταλμένες αρχές. Ειδικά για τα δύο τελευταία είδη ελέγχων, η πρόσβαση ισχύει όταν αυτοί γίνονται εντός του ίδιου κράτους μέλους.

Δικαίωμα πρόσβασης και αναζήτησης στο SIS II έχουν και οι εθνικές δικαστικές αρχές στο πλαίσιο ποινικής δίωξης ή ανακριτικής διαδικασίας. Ο κατάλογος με τις αρχές που εξουσιοδοτούνται να κάνουν απευθείας αναζητήσεις δεδομένων στο SIS II αποστέλλεται στην eu-LISA και δημοσιεύεται.

Το άρθρο 41 κατοχυρώνει την πρόσβαση της Europol στα δεδομένα του SIS, για τους σκοπούς που αναφέρθηκαν στα άρθρα 26, 36 και 38. Είναι σημαντικό ότι εφόσον μετά την αναζήτηση που διενεργεί, εντοπιστεί η ύπαρξη καταχώρισης στο SIS II, η Europol οφείλει να ενημερώσει το καταχωρούν κράτος-μέλος και να πάρει τη συγκατάθεσή του. Η Europol θα καθορίσει τη διαδικασία εξέτασης των δεδομένων εφόσον το κράτος επιτρέψει να χρησιμοποιηθούν αυτά. Φυσικά και η διαβίβαση δεδομένων σε τρίτα μέρη χρήζει συγκατάθεσης από το ενδιαφερόμενο κράτος. Η συγκατάθεση είναι λοιπόν η νομιμοποιητική βάση επεξεργασίας των δεδομένων κάτι το οποίο προβλέπεται και στον ΓΚΠΔ.

Για την ασφάλεια των δεδομένων και την τήρηση των κανόνων επεξεργασίας και των αρχών οι οποίες διέπουν αυτήν, το άρθρο 41 αναφέρει πως η Europol οφείλει να:

«α) καταγράφει κάθε πρόσβαση και αναζήτηση, σύμφωνα με τις διατάξεις του άρθρου 12·

β) με την επιφύλαξη των παραγράφων 3 και 4, δεν συνδέει μέρη ούτε μεταφέρει δεδομένα του SIS II στα οποία έχει πρόσβαση σε οποιοδήποτε ηλεκτρονικό σύστημα συλλογής και επεξεργασίας δεδομένων το οποίο διαχειρίζεται η Europol ή λειτουργεί σε αυτήν, δεν μεταφορτώνει ούτε αντιγράφει μέρη του SIS II σε άλλα αρχεία δεδομένων·

γ) περιορίζει την πρόσβαση στα δεδομένα που έχουν καταχωρισθεί στο SIS II στο ειδικά εξουσιοδοτημένο προσωπικό της Europol·

δ) λαμβάνει και εφαρμόζει τα μέτρα που προβλέπονται στα άρθρα 10 και 11·

ε) επιτρέπει στην κοινή εποπτική αρχή, η οποία συνεστήθη δυνάμει του άρθρου 24 της σύμβασης Europol, να επιβλέπει τις δραστηριότητες της Europol κατά την άσκηση του δικαιώματός της για πρόσβαση και αναζήτηση σε δεδομένα που έχουν εισαχθεί στο SIS II.»

Όμως πρόσβαση στα δεδομένα του SIS II αποκτά με το άρθρο 42 και η Eurojust. Διευκρινίζεται βέβαια στην παράγραφο 6 του άρθρου πως η πρόσβαση σε αυτή επιτρέπεται μόνο στα εθνικά μέλη και τους βοηθούς τους και όχι σε όλο το προσωπικό της Eurojust. Και σε αυτή την περίπτωση βέβαια, όπως και στην Europol, ισχύει η συγκατάθεση του καταχωρούντος κράτους μέλους ως νομιμοποιητική βάση για την χρήση των πληροφοριών που πού εντοπίζονται από την Eurojust. Κάθε αναζήτηση και πρόσβαση καταγράφεται με τα στοιχεία του προσώπου που είχε πρόσβαση. Και στην περίπτωση της Eurojust δεν επιτρέπεται η συλλογή και επεξεργασία δεδομένων από το SIS II και η μεταφορά τους σε άλλη βάση δεδομένων, ενώ ισχύουν κι εδώ τα μέτρα των άρθρων 10 και 11 της ίδιας απόφασης, σχετικά με τη διασφάλιση ασφάλειας και της εμπιστευτικότητας.

Τέλος σύμφωνα με τον κανονισμό (ΕΚ) 1986/2006 «σχετικά με την πρόσβαση στο Σύστημα Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) των υπηρεσιών των κρατών μελών που είναι υπεύθυνες για την έκδοση αδειών κυκλοφορίας οχημάτων», πρόσβαση στα δεδομένα που καταχωρούνται στο SIS II και μάλιστα για αντικείμενα του άρθρου 38 (οχήματα) είναι οι αρχές που είναι αρμόδιες για την έκδοση αδειών κυκλοφορίας οχημάτων αποκλειστικά και μόνο για τον έλεγχο περίπτωσης κλοπής, υπεξαίρεσης, απώλειας των οχημάτων για τα οποία πρόκειται να εκδώσουν άδεια κυκλοφορίας, η αναζήτησής τους ως αποδεικτικά στοιχεία στα πλαίσια ποινικής διαδικασίας. Απευθείας πρόσβαση στα δεδομένα έχουν μόνον οι αρμόδιες κρατικές αρχές. Εάν για κάποιο λόγο η αδειοδότηση οχημάτων γίνεται από μη κρατικό φορέα, τότε αυτός δεν μπορεί να έχει πρόσβαση στα δεδομένα πάρα μόνο διαμέσου της αρμόδιας κρατικής αρχής του άρθρου 40.

#### ▪ *Επεξεργασία Δεδομένων*

Τα άρθρα 46, 47 και 48 επικεντρώνονται στην επεξεργασία των δεδομένων του SIS II. Σύμφωνα με το άρθρο 48 μόνο το καταχωρούν κράτος έχει δικαίωμα τροποποίησης, συμπλήρωσης, διόρθωσης, ενημέρωσης ή διαγραφής των δεδομένων που έχει εισάγει. Ακόμη και αν ένα άλλο κράτος-μέλος εντοπίσει κάποιο πρόβλημα στην ποιότητα των δεδομένων, δεν μπορεί να προχωρήσει μόνο του στην επεξεργασία, αλλά οφείλει να ενημερώσει το καταχωρούν κράτος το οποίο με τη σειρά του θα επαληθεύσει την πληροφορία και, εάν είναι απαραίτητο, θα προβεί στις κατάλληλες ενέργειες.

Μάλιστα σύμφωνα με το άρθρο 46 τα κράτη μέλη μπορούν να επεξεργάζονται τα δεδομένα μόνο για τους σκοπούς που καθορίζονται για κάθε κατηγορία καταχωρίσεων

ενώ η αναπαραγωγή αυτών επιτρέπεται μόνο για τεχνικούς λόγους χωρίς όμως τα αντίγραφα να αποθηκεύονται σε άλλα αρχεία δεδομένων. Τα τεχνικά αντίγραφα αυτά μπορούν να διατηρηθούν μόνο έως 48 ώρες με πιθανή παράταση μόνο σε κατάσταση εκτάκτου και μέχρι αυτή να παρέλθει. Εξαιρέση αποτελούν και μπορούν να διατηρηθούν, σύμφωνα με το άρθρο 47, δεδομένα τα οποία το ίδιο το κράτος έχει καταχωρήσει στο σύστημα ή αφορούν υποθέσεις για τις οποίες το κράτος έχει αναλάβει δράση στο έδαφός του.

Εξαιρετικά σημαντική είναι η 5η παράγραφος του άρθρου 46 όπου διευκρινίζεται πως η επεξεργασία των δεδομένων πρέπει να γίνεται μόνο για το σκοπό για τον οποίο καταχωρίστηκαν. Η εκ νέου επεξεργασία στη βάση διαφορετικού σκοπού θα πρέπει να δικαιολογείται απόλυτα με τη σύνδεση των υποθέσεων, είτε να δικαιολογείται για λόγους σοβαρής απειλής, δημοσίου συμφέροντος και δημόσιας ασφαλείας.

#### ▪ *Δικαιώματα Υποκειμένου*

Στο δωδέκατο κεφάλαιο της απόφασης 2007/5 33/ΔΕΥ, όπου γίνεται πρόβλεψη για την προστασία των δεδομένων, περιλαμβάνονται και τα δικαιώματα του υποκειμένου των δεδομένων. Αυτή η αντίθεση μεταξύ της αποθήκευσης των προσωπικών δεδομένων στο σύστημα αλλά και του υποκειμένου που κατοχυρώνει δικαιώματα αυτών, λειτουργεί και ως ένας άλλος τρόπος ελέγχου της δράσης των αρμοδίων αρχών, έτσι ώστε το δικαίωμα στην προστασία των προσωπικών δεδομένων να μην παραβιαστεί.

Στο άρθρο 58 της απόφασης λοιπόν, προσδιορίζεται πώς το υποκείμενο έχει δικαιώματα πρόσβασης, διόρθωσης εσφαλμένων δεδομένων και διαγραφής δεδομένων που δεν έχουν εισαχθεί ή δεν διατηρούνται νομότυπα. Βέβαια η άσκηση του δικαιώματος πρόσβασης ασκείται σύμφωνα με την εθνική νομοθεσία των κρατών μελών στα οποία γίνεται το αίτημα και η εθνική εποπτική αρχή, σύμφωνα πάντα με το εθνικό δίκαιο, αποφασίζει τον τρόπο ανακοίνωσης των πληροφοριών που ζητήθηκαν. Για να ανακοινώσει ένα κράτος-μέλος, που δεν είναι το καταχωρούν κράτος, πληροφορίες οφείλει πρώτα να ενημερώσει το ενδιαφερόμενο κράτος μέλος, ώστε εκείνο να διατυπώσει τη θέση του μέσω ανταλλαγής συμπληρωματικών δεδομένων. Δεν ανακοινώνονται σε καμία περίπτωση δεδομένα που αφορούν τρίτο πρόσωπο και περιέχονται στην καταχώριση, για λόγους προστασίας των δικαιωμάτων τρίτου προσώπου.

Όσον αφορά την πρόσβαση ο ενδιαφερόμενος οφείλει να ενημερωθεί από τις αρμόδιες αρχές το αργότερο σε 60 μέρες από την υποβολή του αιτήματος, ενώ το χρονικό διάστημα ανέρχεται σε τρεις μήνες για την περίπτωση διόρθωσης ή διαγραφής δεδομένων. Το υποκείμενο των δεδομένων έχει το δικαίωμα προσφυγής και απαίτησης αποζημίωσης σχετικά με καταχώριση που το αφορά. Μπορεί να προσφύγει δυνάμει του εθνικού δικαίου αλλά και ενώπιον του Ευρωπαϊκού Δικαστηρίου. Τα κράτη μέλη οφείλουν να εκτελούν τις δικαστικές αποφάσεις.

## **B.7. Γενικές Παρατηρήσεις**

Το SIS II διευρύνει τη λειτουργία του σε σχέση με την προηγούμενη έκδοσή του, καθώς επεκτείνει τα είδη των καταχωρίσεων και σε αντικείμενα και οχήματα, προσθέτει νέα δεδομένα που μπορούν να αποθηκεύονται για τους σκοπούς των αναζητήσεων. Μάλιστα κάποια από αυτά τα δεδομένα αποτελούν βιομετρικά στοιχεία, δηλαδή προσωπικά δεδομένα ειδικών κατηγοριών, για τα οποία μπορεί ακόμη να μην είναι εφικτή η επεξεργασία τους λόγω ελλιπούς τεχνικής υποδομής, στο μέλλον όμως θα πρωταγωνιστήσουν και θα εμπλουτιστούν με περαιτέρω δεδομένα όπως προφίλ DNA και αποτυπώματα παλάμης. Από αυτήν την διεύρυνση των βάσεων αλλά και τη συμμετοχή πλέον περισσότερων οργανισμών στη βάση SIS, – στο SIS II συμμετέχουν η Europol και Eurojust – είναι δυνατόν να επέλθουν κίνδυνοι σχετικά με το δικαίωμα στην ιδιωτική ζωή που θα συζητηθούν αναλυτικότερα στα συμπεράσματα αυτής της πραγμάτευσης.

Παρόλα αυτά δεν γίνεται να μην λεχθεί πως τα πλεονεκτήματα του ΧΕΑΔ εξασφαλίζονται πλέον με όλο και περισσότερα και αυστηρότερα μέτρα για την εσωτερική και εξωτερική ασφάλεια. Οποσδήποτε οι εξελίξεις των τελευταίων ετών οδήγησαν σε αυτό, όμως διαφαίνεται ο κίνδυνος ο ΧΕΑΔ να αντιμετωπίζεται πλέον ως ένας χώρος περισσότερο αποκλεισμού εισόδου και διαμονής και υποχώρησης θεμελιωμένων δικαιωμάτων έναντι την ασφάλειας. Όσον αφορά στα προσωπικά δεδομένα, το θεσμικό πλαίσιο που παρουσιάστηκε δείχνει προσπάθεια για την προστασία τους. Μάλιστα το γεγονός ότι η ΕΕ μερίμνησε και για την έκδοση του 1725/2018/ΕΕ αλλά και έχει φροντίσει για την λειτουργία ανεξάρτητων εποπτικών αρχών ώστε να προστατεύονται με κάθε τρόπο τα δικαιώματα του υποκειμένου των δεδομένων, καταδεικνύει την ανάγκη για μία ισχυρή νομοθετική βάση που θα λειτουργεί ως ασπίδα σε πιθανούς κινδύνους που προαναφέρθηκαν.

## Γ. Νομολογία και Γνωμοδοτήσεις

Το ζήτημα των δικαιωμάτων του ανθρώπου, της προστασίας των προσωπικών του δεδομένων στα πλαίσια του ΧΕΑΔ εντοπίζεται και στη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (ΔΕΕ) αλλά και σε γνωμοδοτήσεις και αποφάσεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), μέρος των οποίων θα παρουσιαστούν στην συνέχεια. Βέβαια λόγω του πρόσφατου χρονικά ΓΚΠΔ, η πλειοψηφία των υποθέσεων δεν τον χρησιμοποιεί ως νομική βάση. Ωστόσο οι αποφάσεις λειτουργούν ενδεικτικά σχετικά με το θέμα.

### Γ.1. Νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης

Οι ακόλουθες αποφάσεις του ΔΕΕ είναι βέβαια ενδεικτικές της προστασίας των δικαιωμάτων στο δίκαιο της Ένωσης και, ακόμη και αν δεν αφορούν άμεσα το νέο θεσμικό πλαίσιο και την διαχείριση των δεδομένων από όργανα και θεσμούς της ΕΕ εντός της ζώνης Σένγκεν, καταδεικνύουν την αντίληψη της Ένωσης περί προστασίας τους και του καθορισμού των προϋποθέσεων υποχώρησής τους ενώπιον του σκοπού επεξεργασίας στη βάση της αρχής της αναλογικότητας.

#### *Γ.1.α. Απόφαση C-92/09 και C-93/09 (EU:C:2010:662)*

Σύμφωνα με το κείμενο της απόφασης C-92/09 και C-93/09 (EU:C:2010:662) «το ομόσπονδο κράτος της Έσσης στην Γερμανία προχώρησε σε δημοσίευση στον διαδικτυακό τόπο της Ομοσπονδιακής Υπηρεσίας Γεωργίας και Διατροφής δεδομένων προσωπικού χαρακτήρα των δικαιούχων κονδυλίων που αφορούσαν γεωργικές εκμεταλλεύσεις, από το Ευρωπαϊκό Γεωργικό Ταμείο Εγγυήσεων. Τα υποκείμενα των δεδομένων αντιτάχθηκαν σε αυτές τις δημοσιεύσεις καθώς, δεν δικαιολογούνταν από λόγους υπέρτερου δημοσίου συμφέροντος. Το ομόσπονδο κράτος της Έσσης θεωρούσε, από την πλευρά του, ότι η δημοσίευση των δεδομένων ήταν υποχρεωτική. Στο πλαίσιο αυτό, το Verwaltungsgericht Wiesbaden (διοικητικό πρωτοδικείο του Wiesbaden, Γερμανία) υπέβαλε στο Δικαστήριο αρκετά ερωτήματα σχετικά με το κύρος ορισμένων διατάξεων του κανονισμού (ΕΚ) 1290/2005 και με το κύρος του κανονισμού (ΕΚ) 259/2008, οι οποίοι επιβάλλουν τη δημοσιοποίηση τέτοιων πληροφοριών, ιδίως μέσω των διαδικτυακών τόπων των αντίστοιχων εθνικών υπηρεσιών.»

Όπως έγινε αποδεκτό «όσον αφορά τη **στάθμιση μεταξύ του δικαιώματος προστασίας των δεδομένων προσωπικού χαρακτήρα**, το οποίο αναγνωρίζεται από τον

Χάρτη, και της υποχρέωσης διαφάνειας όσον αφορά τα ευρωπαϊκά ταμεία, η δημοσίευση σε διαδικτυακό τόπο ονομαστικών πληροφοριών σχετικά με τους δικαιούχους των κονδυλίων και τα ποσά που έχουν εισπράξει συνιστά, δεδομένης της ελεύθερης πρόσβασης των τρίτων στον διαδικτυακό τόπο, επέμβαση στο δικαίωμα σεβασμού της ιδιωτικής ζωής των ενδιαφερόμενων δικαιούχων, γενικά, και προστασίας των δεδομένων προσωπικού χαρακτήρα που τους αφορούν, ειδικά (σκέψεις 56-64)». Μία τέτοια επέμβαση όπως αναφέρεται στην συνέχεια δικαιολογείται μόνο τηρώντας την αρχή της αναλογικότητας.

Με την απόφαση αυτή διαφαίνεται η συμβατότητα του παράγωγου δικαίου της Ένωσης με το δικαίωμα προστασίας των προσωπικών δεδομένων καθώς, αν και το Δικαστήριο υπερασπίστηκε το δικαίωμα στην διαφανή ενημέρωση όλων των φορολογούμενων, κατά την στάθμιση αυτού με το δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα απεφάνθη πως οι διατάξεις των κανονισμών βάσει των οποίων έγινε η δημοσίευση είναι «ανίσχυρες λόγω της μη ανταπόκρισης των έκθεσης των δεδομένων με το σκοπό της δημοσίευσης». Δίνεται λοιπόν ιδιαίτερη σημασία στο δικαίωμα στην ιδιωτική ζωή, το οποίο περιέχει και το δικαίωμα την προστασία των προσωπικών δεδομένων. Η αρχή της αναλογικότητας είναι κεντρική για την στάθμιση όταν εντοπίζονται ανομοιομορφίες κατά την εφαρμογή της νομοθεσίας.

### ***Γ.1.β Απόφαση C-291-12, EU:C:2013:670***

Το δικαίωμα βέβαια στην προστασία των προσωπικών δεδομένων δεν υπερέχει κάθε διάταξης και κρίνεται αναλογικά προς το σκοπό της συλλογής τους. Όπως αναφέρεται στα πραγματικά περιστατικά της απόφασης C-291-12, EU:C:2013:670 «ο M. Schwarz ενώ είχε ζητήσει από τον δήμο του Bochum (Γερμανία) την έκδοση διαβατηρίου, δεν ήθελε όμως να αφήσει να του πάρουν τα δακτυλικά του αποτυπώματα και ο δήμος απέρριψε την αίτησή του, προσέφυγε στο ΔΕΕ ζητώντας να υποχρεωθεί ο δήμος να του χορηγήσει διαβατήριο χωρίς λήψη των δακτυλικών του αποτυπωμάτων, αμφισβητώντας το κύρος του αντίστοιχου κανονισμού (ΕΚ) 2252/2004 που καθιέρωσε την υποχρεωτική λήψη των δακτυλικών αποτυπωμάτων των αιτούντων την έκδοση διαβατηρίου και επικαλούμενος την παραβίαση των προσωπικών του δεδομένων και του δικαιώματός του στην ιδιωτική ζωή».

Το Δικαστήριο έκρινε ότι, «μολονότι η λήψη και η διατήρηση δακτυλικών αποτυπωμάτων από τις εθνικές αρχές, όπως διέπονται από το άρθρο 1, παράγραφος 2, του κανονισμού (ΕΚ) 2252/2004, συνιστούν επέμβαση στα δικαιώματα σεβασμού της



ιδιωτικής ζωής και προστασίας των δεδομένων προσωπικού χαρακτήρα, **η επέμβαση αυτή δικαιολογείται από τον σκοπό προστασίας των διαβατηρίων έναντι κάθε δόλιας χρήσης τους**». Μάλιστα τονίσθηκε πως ο νομός αυτός αποτελεί αναγνωρισμένο από την ΕΕ σκοπός γενικού συμφέροντος εφόσον αποσκοπεί στην αποτροπή παράνομης εισόδου και απειλής στην ΕΕ. Άρα κρίθηκε αναλογικό και αναγκαίο μέτρο προς τον επιδιωκόμενο σκοπό.

Φαίνεται κι εδώ πως η αρχή της αναλογικότητας αποτελεί βασική αρχή διάκρισης των ορίων παραβίασης των προσωπικών δεδομένων και ως εκ τούτου διαδραματίζει κεντρικό ρόλο για την διαχείριση των προσωπικών δεδομένων στα συστήματα πληροφοριών της ένωσης σύμφωνα και με το νέο ΓΚΠΔ.

#### ***Γ.1.γ Η απόφαση C-582/14, EU:C:2016:779***

Η απόφαση Breyer (C-582/14, EU:C:2016:779) καταδεικνύει πως η έννοια των προσωπικών δεδομένων ακόμα και όταν δεν οδηγούν σε ταυτοποίηση, εξακολουθεί να ισχύει και πρέπει να προστατεύεται.

Στο κείμενο της απόφασης αναφέρεται πως «Ο P. Breyer είχε ασκήσει, ενώπιον των γερμανικών πολιτικών δικαστηρίων, αγωγή παράλειψης κατά της Ομοσπονδιακής Δημοκρατίας της Γερμανίας για να την υποχρεώσει να παύσει να αποθηκεύει ή να αναθέτει σε τρίτους την αποθήκευση δεδομένων πληροφορικής που διαβιβάζονταν μετά το πέρας κάθε επίσκεψης στους διαδικτυακούς τόπους των γερμανικών ομοσπονδιακών υπηρεσιών, όπου με σκοπό την αποτροπή επιθέσεων και τη διευκόλυνση της ποινικής δίωξης των «χάκερς», ο φορέας παροχής υπηρεσιών τηλεμέσων των γερμανικών ομοσπονδιακών υπηρεσιών κατέγραφε κάποια δεδομένα, όπως τη «δυναμική» διεύθυνση IP, με την οποία βέβαια δεν μπορεί να επέλθει ταυτοποίηση από τον ίδιο τον φορέα παροχής αλλά ο πάροχος πρόσβασης στο διαδίκτυο διέθετε, από την πλευρά του, πρόσθετες πληροφορίες οι οποίες, εάν συνδυάζονταν με τη διεύθυνση IP, καθιστούσαν δυνατή την εξακρίβωση της ταυτότητας του χρήστη.» **Η κρίση του ΔΕΕ** βασίστηκε στην οδηγία 95/46/EK – η οποία έχει πλέον αντικατασταθεί με τον ΓΚΠΔ – και **χαρακτήρισε την δυναμική διεύθυνση IP ως προσωπικό δεδομένο ακόμα και αν δεν οδηγεί στην άμεση ταυτοποίηση.**

#### ***Γ.1.δ Η απόφαση C-524/06, EU:C:2008:724***

Με την απόφαση της υπόθεσης Huber (C-524/06, EU:C:2008:724), θίγεται το θέμα της διατήρησης δεδομένων και για στατιστικούς λόγους κάτι το οποίο επιτρέπεται

κατά τον 1986/2007, οφείλουν όμως τα δεδομένα να είναι τα απολύτως αναγκαία για τους σκοπούς της επεξεργασίας.

Το ΔΕΕ απεφάνθη αναλόγως πως **η επεξεργασία** δεδομένων προσωπικού χαρακτήρα, η οποία γινόταν στο πλαίσιο της λειτουργίας του μητρώου από την Ομοσπονδιακή Υπηρεσία Μετανάστευσης και Προσφύγων στην Γερμανία ήταν **σύμφωνη με το δίκαιο της Ένωσης όσο αφορά τη διατήρηση ενός τέτοιου μητρώου για λόγους ασφάλειας**. «Εντούτοις, ένα τέτοιο μητρώο δεν μπορεί να περιέχει άλλες πληροφορίες πλην εκείνων που είναι αναγκαίες για τον σκοπό αυτό, κατά την έννοια της οδηγίας για την προστασία των δεδομένων προσωπικού χαρακτήρα (σκέψεις 54, 58, 59). Εν πάση περιπτώσει, δεν μπορούν να θεωρηθούν αναγκαίες, υπό την έννοια του άρθρου 7, στοιχείο ε΄, της οδηγίας 95/46/ΕΚ, η αποθήκευση και η επεξεργασία ονομαστικών δεδομένων προσωπικού χαρακτήρα στο πλαίσιο ενός τέτοιου μητρώου για λόγους στατιστικής (σκέψεις 52, 66, 68). Μάλιστα η διαχείριση των δεδομένων εξαρτάται και από την εθνική νομοθεσία των κρατών μελών και στην απόφαση C-468/10 και C-469/10, EU:C:2011:777, το Δικαστήριο κατέληξε στο συμπέρασμα ότι το άρθρο 7, στοιχείο στ΄, της οδηγίας 95/46/ΕΚ απαγορεύει σε κράτος μέλος να αποκλείει κατηγορηματικώς και γενικώς τη δυνατότητα επεξεργασίας ορισμένων κατηγοριών δεδομένων προσωπικού χαρακτήρα, χωρίς να επιτρέπει στάθμιση των αντικρουόμενων δικαιωμάτων και συμφερόντων στο πλαίσιο συγκεκριμένης περίπτωσης (σκέψεις 47, 48)».

## **Γ.2. Γνωμοδοτήσεις και Αποφάσεις της Αρχής Δεδομένων Προσωπικού Χαρακτήρα.**

### ***Γ.2.α. Γνωμοδότηση 3/2010 και αποφάσεις που την στηρίζουν***

Από την ιστοσελίδα της ΑΠΔΠΧ αντλήθηκε η μοναδική γνωμοδότηση που ερμηνεύει τις κρίσιμες διατάξεις για την καταχώριση και διαγραφή αλλοδαπών από το Σύστημα Πληροφοριών Σένγκεν και τον Εθνικό Κατάλογο Ανεπιθύμητων Αλλοδαπών. Βέβαια και πάλι η νομοθετική βάση των αποφάσεων δεν περιλαμβάνει τον ΓΚΠΔ.

Η γνωμοδότηση 3/2010 προέκυψε αφού η Αρχή συνεδρίασε προκειμένου να γνωμοδοτήσει σχετικά με τις νόμιμες προϋποθέσεις καταχώρισης και διαγραφής αλλοδαπών από το Σύστημα Πληροφοριών Σένγκεν. Στο δεύτερο σημείο της γνωμοδότησης κρίνει «ότι η καταχώριση στο ΣΠΣ λαμβάνει χώρα βάσει μίας εθνικής καταχώρισης, η οποία έχει έρεισμα στις αποφάσεις των αρμοδίων διοικητικών αρχών και δικαστηρίων». Επίσης «Τα κριτήρια και η διαδικασία εγγραφής και διαγραφής

αλλοδαπών από τον κατάλογο ανεπιθύμητων αλλοδαπών καθορίζονται με απόφαση των Υπουργών Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης, Εξωτερικών, Εθνικής Άμυνας, Δικαιοσύνης και Δημοσίας Τάξης». Παρόλα αυτά καταλήγει πως δεν είναι αυτοδίκαιη η καταχώριση στο ΣΠΣ κάθε προσώπου που εγγράφεται σε αυτόν τον κατάλογο. Η καταχώριση στο ΣΠΣ επιτρέπεται μόνον όταν πληρούνται οι προϋποθέσεις του άρθρου 96 της ΣΕΣΣ.

Σχετικά με την διατήρηση των δεδομένων που έχει καταχωρίσει η χώρα στο SIS, ο χρόνος διατήρησής τους βασίζεται στο άρθρο 112 της ΣΕΣΣ που ορίζει ότι: «1. Τα δεδομένα προσωπικού χαρακτήρα που έχουν καταχωρισθεί στο Σύστημα Πληροφοριών Σένγκεν για την αναζήτηση προσώπων, διατηρούνται μόνον όσο χρονικό διάστημα είναι απαραίτητο για την επίτευξη του επιδιωκόμενου σκοπού. Το αργότερο τρία χρόνια μετά την καταχώρισή τους σε αρχείο, η αναγκαιότητα διατηρήσεώς τους πρέπει να εξετάζεται από το καταχωρούν Συμβαλλόμενο Μέρος. Για τις καταχωρίσεις του άρθρου 99 η προθεσμία αυτή διαρκεί ένα έτος». Επίσης αναγνωρίζει πως η έλλειψη αιτιολογημένης απόφασης για την αναγκαιότητα διατήρησης της καταχώρισης καθιστά την καταχώριση παράνομη και διαγραφτέα, σύμφωνα και με την Κοινή Αρχή Ελέγχου. Έτσι με την πάροδο της τριετίας από την καταχώριση στο SIS II, και χωρίς αιτιολογημένη απόφαση διατήρησης της εγγραφής, η καταχώριση διαγράφεται.

Φαίνεται πως η γνωμοδότηση της ΑΠΔΠΧ τοποθετείται επί των διατάξεων του 1986/2007 και της απόφασης 2007/533/ΕΕ και εναρμονίζεται με τη σχετική Ευρωπαϊκή νομοθεσία στα σημεία που άφηνε στην διακριτική ευχέρεια των κρατών μελών θέματα σχετικά με τη διαχείριση των εγγραφών. Επιπλέον διευκρινίζει πως:

«α) δικαστική ή διοικητική απέλαση κατ' εφαρμογήν της εθνικής νομοθεσίας για την είσοδο και διαμονή υπηκόων τρίτων χωρών στην ελληνική επικράτεια δικαιολογεί την καταχώριση του αλλοδαπού και στους δύο καταλόγους

β) καταδίκη αλλοδαπού από εθνικό δικαστήριο σε αδίκημα, για το οποίο προβλέπεται ποινή τουλάχιστον ενός (1) έτους, συνιστά λόγο εγγραφής στο ΣΠΣ

γ) αποχρώσες ενδείξεις για διάπραξη ή προπαρασκευαστικές ενέργειες αξιόποινης πράξης, για την οποία προβλέπεται ποινή τουλάχιστον ενός (1) έτους, δικαιολογούν την εγγραφή στο ΣΠΣ, εφόσον η πράξη αξιολογείται ότι συνιστά απειλή της δημόσιας τάξης και ασφάλειας».

Η γνωμοδότηση αυτή υποστηρίζεται με μία σωρεία αποφάσεων που εκδόθηκαν και οι οποίες ενέκριναν το δικαίωμα διαγραφής αλλοδαπών από το SIS II εφόσον

συνέτρεχαν οι παραπάνω προϋποθέσεις (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2020).

### *Γ.2.β Αποφάσεις σχετικά με διαγραφή από SIS λόγω διαγραφής από ΕΚΑΝΑ.*

Οι αποφάσεις της ΑΠΔΠΧ υπ' αριθμ. 93/2002, 56/2004, 65/2005, 77/2005 και 53/2006, κάνουν φανερό τον τρόπο αντιμετώπισης του δικαιώματος διαγραφής (δικαίωμα στη λήθη) από τον Εθνικό Κατάλογο Ανεπιθύμητων Αλλοδαπών (ΕΚΑΝΑ) και τη συνεπακόλουθη διαγραφή από το ΣΠΣ.

Κοινό σημείο όλων των αποφάσεων είναι πως το υποκείμενο των δεδομένων ζητεί την διαγραφή του από τον ΕΚΑΝΑ και από το ΣΠΣ. Σε όλες τις περιπτώσεις πρόκειται για αλλοδαπούς που ενώ είχαν υποστεί διοικητική ή δικαστική απέλαση, επανήλθαν παράνομα στην χώρα και δυνάμει της τότε ισχύουσας νομοθεσίας εξέδωσαν άδεια παραμονής από τους οικείους δήμους. Παρόλα αυτά, η εγγραφή τους στον ΕΚΑΝΑ και στο ΣΠΣ παρέμενε ακόμα και μετά την πάροδο τριετίας χωρίς ουσιαστική αιτιολόγηση. Όταν για διαφορετικές αιτίες συνελήφθησαν και λόγω των καταχωρίσεων στους δύο αυτούς καταλόγους δεν επετράπη η είσοδός τους στη χώρα ή η επέκταση της άδεια παραμονής τους αλλά απορρίφθηκε και η αίτηση τους για διαγραφή των δεδομένων τους από τους καταλόγους από το Υπουργείο Εσωτερικών, προσέφυγαν στην ΑΠΔΠΧ.

Η Αρχή επικαλούμενη στο σκεπτικό των αποφάσεων εθνική νομολογία σύμφωνα με την οποία επιτρεπόταν η έκδοση άδειας παραμονής «σε αλλοδαπούς που διαμένουν παράνομα στην Ελλάδα, εφόσον αποδείξουν ότι διαμένουν στη χώρα, νόμιμα ή παράνομα, συνεχώς επί ένα έτος μέχρι την έναρξη ισχύος του παρόντος»(απόφαση 65/2005) . Παράλληλα αναφερόμενη στον ίδιο νόμο συνεχίζει «η καταχώριση αλλοδαπού στον κατάλογο ανεπιθύμητων συνεπεία διοικητικής απέλασης ή για οποιαδήποτε άλλη αιτία, για παράνομη είσοδο, έξοδο, παραμονή ή εργασία στο ελληνικό έδαφος, ο οποίος έχει λάβει την άδεια παραμονής της παρ. 1 του άρθρου 66 του Ν. 2910/2001 και εφόσον στηρίζεται σε γεγονότα που έγιναν σε χρόνο προγενέστερο της έκδοσης της ανωτέρω άδειας παραμονής, **δεν συνεπάγεται έναντι των κατόχων της οποιαδήποτε έννομο αποτέλεσμα και επέρχεται, αυτοδικαίως, διαγραφή τους από τον ίδιο κατάλογο**».

Έτσι καταλήγει πως καταδικαστικές αποφάσεις προγενέστερες του χρόνου έκδοσης της άδειας διαμονής, δεν δικαιολογούν την διατήρηση της καταχώρισης στον ΕΚΑΝΑ, από όπου αποφασίζει τη διαγραφή τους. Συνεπακόλουθα και εφόσον έχει παρέλθει και τριετία από την εγγραφή τους και δεν υπάρχει απόφαση που να αιτιολογεί

την διατήρηση της καταχώρισης στο ΣΠΣ, αποφασίζει και την διαγραφή από αυτόν τον κατάλογο.

## **Δ. Τελικά Συμπεράσματα**

### **Δ.1. Κριτική Θεώρηση της Προστασίας Προσωπικών Δεδομένων στο SIS II**

Το Σύστημα Πληροφοριών Σένγκεν, από τη σύστασή του, αποτέλεσε ένα αποδοτικό και αποτελεσματικό εργαλείο εξασφάλισης της ελευθερίας και της ασφάλειας στο χώρο Σένγκεν, αντιμετωπίζοντας το διασυνοριακό οργανωμένο έγκλημα. Μέχρι και σήμερα παραμένει ένα από τα μεγαλύτερα συστήματα πληροφοριών μεγάλης κλίμακας, ενισχύει τον έλεγχο στα εξωτερικά σύνορα του ΧΕΑΔ αλλά και τη συνεργασία μεταξύ των κρατών μελών του χώρου. Φυσικά ανταποκρινόμενο στις τεχνολογικές εξελίξεις αλλά και τις νέες προκλήσεις στο χώρο της ασφάλειας, μετανάστευσης και δικαιοσύνης, έπρεπε και αυτό να εξελιχθεί. Έτσι βαθμιαία διαμορφώθηκε το Σύστημα Πληροφοριών Σένγκεν δεύτερης γενιάς, με μεγαλύτερη δυνατότητα υποστήριξης και αποθήκευσης δεδομένων για όλα τα κράτη-μέλη. Παράλληλα περισσότεροι οργανισμοί (Europol, Eurojust) απέκτησαν πρόσβαση σε αυτό στοχεύοντας πάντα στην αποδοτικότερη και αποτελεσματικότερη λειτουργία του για τη διατήρηση της ασφάλειας.

Η διαδικασία ανάπτυξης του SIS II, προήλθε από σταδιακές τροποποιήσεις των κανόνων που ορίζονται από την ΣΕΣΣ. Δεν έγινε δηλαδή προσπάθεια ανάπτυξης από την αρχή ενός νέου και ενιαίου νομικού πλαισίου. Αποτέλεσμα αυτού είναι η πολυπλοκότητα της νομοθετικής του βάσης, αφού ουσιαστικά αυτή αποτελείται από δύο κανονισμούς και μία απόφαση (κανονισμοί 1986 /2006, 1987/2006 και απόφαση 533/2007/ΔΕΥ), τα οποία ρυθμίζουν το πλαίσιο και τους κανόνες λειτουργίας του SIS II αλλά και τα θέματα περί προσωπικών δεδομένων που καταχωρούνται σε αυτό. Ιδιαίτερα για τα θέματα των προσωπικών δεδομένων η έκδοση του ΓΚΠΔ και του αντίστοιχου κανονισμού για την προστασία των δεδομένων από ευρωπαϊκά όργανα και οργανισμούς (κανονισμός 1725/2018), επεκτείνουν το νομικό πλαίσιο και συντείνουν στην πολυπλοκότητά του. Συνεπώς, αν και μετά τη συνθήκη της Λισαβόνας ισχύει η διαδικασία της συναπόφασης, που έδινε στο Ευρωπαϊκό κοινοβούλιο τη δυνατότητα να συνδιαμορφώσει τους κανονισμούς, οι προηγούμενες καθυστερήσεις αλλά και η ανάγκη επίσπευσης της υιοθέτησης της συγκεκριμένης νομοθεσίας, είχε ως αποτέλεσμα αυτή να υιοθετηθεί στην πρώτη ανάγνωση μεταξύ Επιτροπής, Συμβουλίου και Προεδρίας (Παπαγιάννης Δ., 2008). Τέλος, αν και ζητήθηκε από τον Ευρωπαϊκό Επόπτη Προστασίας Δεδομένων να εξετάσει τις προτάσεις και να εκφέρει γνώμη, η σύντομη χρονική προθεσμία από τον

δόθηκε ουσιαστικά περιορίσει το ρόλο του και δεν ήταν δυνατή η συνεισφορά του (Parkin J., 2011).

Το 2016 μέσα από την αξιολόγησή της Ευρωπαϊκής Επιτροπής για το SIS II (Ευρωπαϊκό Κοινοβούλιο, 2018), προκύπτει η διάθεση για περαιτέρω βελτίωση της αποδοτικότητας και αποτελεσματικότητας του. Τονίζεται ότι οι πρόσφατες εξελίξεις της προσφυγικής κρίσης έφεραν μεγάλες πιέσεις στα σύνορα, καθώς υπήρξε μεγάλος αριθμός ανθρώπων που θέλησαν να τα περάσουν νόμιμα ή παράνομα. Από το 2014 έως το 2015 ένα εκατομμύριο περισσότεροι πολίτες τρίτων χωρών θέλησαν να εισέλθουν στον ΧΕΑΔ. Μάλιστα εκτιμάται ότι ο αριθμός αυτός θα συνεχίσει να αυξάνεται και από τα 50 εκατομμύρια το 2015, θα αυξηθεί σε 76 εκατομμύρια απόπειρες εισόδου στον ΧΕΑΔ έως το 2025. Αυτή η μεγάλη εισροή οδήγησε, και εν μέσω της προσφυγικής κρίσης, πολλές χώρες να επαναφέρουν τους ελέγχους στα σύνορά τους, καταργώντας στην ουσία με αυτό τον τρόπο την ελεύθερη μετακίνηση. Υπό το φως λοιπόν αυτών των γεγονότων, η Ευρωπαϊκή Επιτροπή υπέβαλε πρόταση για έκδοση τριών κανονισμών που θα αποτελέσουν το νέο νομοθετικό Πλαίσιο για την εξέλιξη του SIS II. Συγκεκριμένα προτείνεται:

« α) Κανονισμός σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του SIS στον τομέα των συνοριακών ελέγχων, ο οποίος θα καταργήσει τον κανονισμό SIS II·

β) Κανονισμός σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του SIS στον τομέα της αστυνομικής συνεργασίας και της δικαστικής συνεργασίας σε ποινικές υποθέσεις, ο οποίος θα καταργήσει, μεταξύ άλλων, την απόφαση SIS II· και

γ) Κανονισμός σχετικά με τη χρήση του SIS για την επιστροφή των παρανόμως διαμενόντων υπηκόων τρίτων χωρών.” (Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, 2019, σελ 395)

Άλλος ένας στόχος που θέτει η επιτροπή είναι η διαλειτουργικότητα των Συστημάτων Πληροφόρησης (SIS II, VIS, EURODAC) τα οποία έως τώρα είναι πολλά και χωρίς εύκολη μεταξύ τους αλληλεπίδραση. Έτσι προσπαθεί να θεραπεύσει την κατακερματισμένη διαχείριση των δεδομένων που γίνεται σε αυτά τα συστήματα. Με την διαλειτουργικότητα αναμένεται οι αρμόδιες αστυνομικές, τελωνειακές και δικαστικές αρχές να έχουν πρόσβαση στις πληροφορίες που είναι αναγκαίες για τα καθήκοντα τους αλλά παράλληλα να διατηρείται και ένα υψηλό επίπεδο προστασίας των δικαιωμάτων των προσωπικών δεδομένων και της ιδιωτικής ζωής. είναι σημαντικό να υπάρξουν οι κατάλληλες εγγυήσεις έτσι ώστε το νέο θεσμικό πλαίσιο αλλά και η διαλειτουργικότητα να εναρμονίζονται με τον ΓΚΠΔ . Μάλιστα στις προτάσεις της η Ευρωπαϊκή

Επιτροπή, θέτει και τη δημιουργία ενός τετάρτου συστήματος διαχείρισης των συνόρων το οποίο θα περιορίζεται σε υπηκόους τρίτων χωρών αλλά και στη δημιουργία ενός συστήματος συλλογής πληροφοριών (Ευρωπαϊκό Σύστημα Πληροφοριών και Αδείας ταξιδιού ETIAS) που θα σχετίζεται για όσους ταξιδεύουν στην ΕΕ χωρίς θεώρηση με στόχο τον έλεγχο της παράνομης μετανάστευσης και την διατήρηση της ασφάλειας (Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, 2019).

Γίνεται λοιπόν φανερό πως η συλλογή δεδομένων στα συστήματα πληροφοριών αποτελεί μία πραγματικότητα έτσι ώστε να διατηρηθεί το κεκτημένο Σένγκεν αποτελεσματικό και αποδοτικό. Όμως η προστασίας των δεδομένων προσωπικού χαρακτήρα παραμένει ακόμα και στο παρόν νομοθετικό πλαίσιο - πόσο μάλλον στη μελλοντική εξέλιξή του - θέμα προβληματισμού. Διαβάζοντας τη γνωμοδότηση του ΕΕΠΔ, αντιλαμβανόμαστε την ανησυχία πως η εισαγωγή νέων κατηγοριών δεδομένων ήδη από το SIS II αλλά και η επέκτασή τους στη διαμόρφωση ενός νέου συστήματος, θέτουν το θέμα της εξέτασής τους υπό το πρίσμα της αρχής της αναλογικότητας και της ελαχιστοποίησης των δεδομένων. Ιδιαίτερα η είσοδος στο σύστημα βιομετρικών στοιχείων χρήζει προσοχής και θα έπρεπε να περιγράφουν με ακρίβεια οι πληροφορίες που θα αποθηκεύονται καθώς μπορεί να εμπλέκονται ειδικών κατηγοριών προσωπικά δεδομένα. Χαρακτηριστικό είναι το παράδειγμα των προβλημάτων υγείας, τα οποία στο πλαίσιο της αποθήκευσης πληροφοριών προφίλ DNA μπορεί να αποκαλύπτονται. Είναι λοιπόν σωστό η επεξεργασία των στοιχείων να γίνεται με προσοχή και να κρατούνται μόνο τα στοιχεία εκείνα που ανταποκρίνονται στο σκοπό της καταχώρισης.

Άλλο ένα σημείο για το οποίο εκδηλώνεται ανησυχία στην ίδια γνωμοδότηση είναι ο όλο και μεγαλύτερος αριθμός των αρχών με δικαιώματα πρόσβασης στις βάσεις δεδομένων του συστήματος. Ήδη στο SIS II κατοχυρώνεται η πρόσβαση στο σύστημα της Europol και Eurojust βάσει της εντολής τους. Αυτό δημιουργεί μία ασάφεια στους σκοπούς πρόσβασης και χρήσης των δεδομένων. Σύμφωνα με την Τζώρτζη Β. (2018), αν και προβλέπεται στη νομική βάση του SIS II πως η επεξεργασία των δεδομένων μπορεί να γίνει μόνο για το σκοπό για τον οποίο έγινε η καταχώριση και πως οι οργανισμοί αυτοί έχουν πρόσβαση στα δεδομένα που τους είναι αναγκαία για την εκτέλεση των καθηκόντων τους, το γεγονός ότι η πρόσβαση εξαρτάται από την εντολή τους που στην ουσία δύναται να τροποποιηθεί, δημιουργεί αυτήν την ασάφεια. Μία τροποποίηση δηλαδή της εντολής μπορεί να οδηγήσει σε τροποποίηση των καθηκόντων της και άρα και των δικαιωμάτων πρόσβασης.



Επιπλέον, οι κανονισμοί προβλέπουν το δικαίωμα ενημέρωσης του υποκειμένου για την καταχώρηση του στο σύστημα, καθώς από αυτό εξαρτάται και η άσκηση των δικαιωμάτων του περί δυνατότητας διόρθωσης ή διαγραφής από το σύστημα. Φαίνεται όμως πως το δικαίωμα αυτό της κατά το δυνατόν ταχύτερης ενημέρωσης δεν προκρίνεται εφόσον δεν υπάρχει δέσμευση περί αυτού. Τίθενται κάποιες προθεσμίες, οι οποίες όμως εξαρτώνται και από την εθνική νομοθεσία κάθε κράτους. Αυτό δύναται να προκαλέσει προβλήματα εάν δεν έχει υπάρξει ενημέρωση του υποκειμένου και παρέλθει το προβλεπόμενο διάστημα για την υποβολή έφεσης ή ακόμα και όταν το υποκείμενο θελήσει να εκδώσει visa Schengen.

Κάτι ακόμα που προβλέπεται για το SIS II είναι η δυνατότητα διασυνδέσεων μεταξύ των καταχωρήσεων αυξάνοντας έτσι την αστυνόμευση και τη διατήρηση της ασφάλειας στο χώρο. Παρόλα αυτά τίθενται ζητήματα σχετικά με τις επιπτώσεις που μπορεί να έχουν οι διασυνδέσεις αναφορικά με την παραβίαση της αρχής της αναλογικότητας και το πιθανό στιγματισμό ανθρώπων. Έτσι, μία διασύνδεση μεταξύ ενός διωκόμενου που έχει καταχωρισθεί στο σύστημα και μελών της οικογένειάς του τα οποία τίθεται στη διακριτική παρακολούθηση, μπορεί να έχει ένα τέτοιο αποτέλεσμα.

Επιπροσθέτως ο ΕΕΠΔ με τη γνωμοδότηση του «ζητεί να παρασχεθεί καλύτερη αιτιολόγηση της παράτασης της περιόδου διατήρησης των δεδομένων για τις καταχωρίσεις σχετικά με πρόσωπα». Πράγματι τα διαστήματα διατήρησης των δεδομένων, αν και ορίζονται από τους συναφείς κανονισμούς, εξαρτώνται και πάλι από το εθνικό δίκαιο των κρατών μελών. Για αυτό ακριβώς το λόγο είναι ανάγκη να υπάρχει λεπτομερής αιτιολόγηση της διατήρησης των δεδομένων στο σύστημα.

Άλλο ένα χαρακτηριστικό της νομικής βάσης του SIS II είναι η συχνή αναφορά σε γενικές ρήτρες δημόσιας τάξης, δημόσιας ασφάλειας και εθνικών συμφερόντων ή αποτροπής απειλής προς τον ΧΕΑΔ. Με αυτήν την αιτιολόγηση μπορούν να γίνουν πολλές εξαιρέσεις όσον αφορά στη συλλογή, επεξεργασία, διατήρηση των δεδομένων στο σύστημα αλλά και περιστολή των δικαιωμάτων του υποκειμένου. Πρόκειται δηλαδή για ευρύτερες κατηγορίες δραστηριοτήτων που μπορεί να εκληφθούν ως απειλητικές προς τη ζώνη Σένγκεν αναλόγως των εκάστοτε συνθηκών και στόχων και μπορεί να εκτείνονται από πραγματική τρομοκρατική απειλή έως διαδηλώσεις διαμαρτυρίας (Παπαγιάννης Δ., 2001)

Τέλος, αυτό το ευρύ πλέγμα διατάξεων που θεσμοθετεί τη λειτουργία των Συστημάτων πληροφοριών, συμπεριλαμβανομένου και του SIS II, έχει ειδικότερες διατάξεις για τα προσωπικά δεδομένα και ειδικά δικαιώματα. Παρόλη την προσπάθεια

με τη θεσμοθέτηση του ΓΚΠΔ αλλά και του αντίστοιχου κανονισμού για τα Ευρωπαϊκά όργανα (1725/2018/ΕΕ), σε ορισμένα σημεία ενδέχεται να υπάρχει σύγκρουση, καθώς στους κανονισμούς για τα προσωπικά δεδομένα δεν προβλέπεται η υπεροχή ειδικότερων διατάξεων που βρίσκονται σε ισχύ. Έτσι η άσκηση βασικών δικαιωμάτων του υποκειμένου όπως αυτό της διόρθωσης είτε διαγράψης δεδομένων του από το εθνικό σύστημα κάποιας χώρας να δικαιολογείται σύμφωνα με τον ΓΚΠΔ ενώ δεν είναι δυνατή σύμφωνα με τους κανόνες λειτουργίας του SIS II.

## **Δ.2. Προτάσεις – Μελλοντικές Προοπτικές**

Στην γνωμοδότηση του ΕΕΠΔ για το 2017 σχετικά με την νέα νομική βάση του SIS, διαπιστώνεται ότι «η πολλαπλότητα των συστημάτων πληροφοριών μεγάλης κλίμακας της ΕΕ οφείλεται στις συγκεκριμένες ανάγκες που πρέπει να αντιμετωπιστούν, με δεδομένες τις εξελίξεις σε θεσμικό, πολιτικό και νομικό πλαίσιο. Η κατάσταση αυτή είχε ως συνέπεια την πολυπλοκότητα των νομικών πλαισίων και των μοντέλων διακυβέρνησης.» (Ευρωπαϊός Επόπτης Προσωπικών Δεδομένων, 2017, σελ.2). Πράγματι όπως προαναφέρθηκε, η πολυπλοκότητα των νομοθετικών ρυθμίσεων και η κατά σημεία έλλειψη εναρμόνισης τους είναι ένα από τα ζητήματα που πρέπει να αντιμετωπιστεί κατά το σχεδιασμό του νέου Συστήματος Πληροφοριών Σένγκεν.

Είναι λοιπόν ανάγκη να εξεταστεί η θέσπιση ενός νομοθετικού πλαισίου ενιαίου και συνεκτικού, το οποίο θα αφορά όλες τις βάσεις δεδομένων της ΕΕ και θα έχουν μία ολοκληρωμένη ενιαία και σύγχρονη αντιμετώπιση για την προστασία των προσωπικών δεδομένων σε αυτές. Είναι δηλαδή σημαντικό να περιοριστεί η επιρροή της εθνικής νομοθεσίας που τώρα προβλέπεται σε αρκετά σημεία των κανονισμών και να υπάρχει ένας κεντρικός σχεδιασμός, απόλυτα ακριβής και περιεκτικός. Σύμφωνα και με τον ΕΕΠΔ πρέπει να δοθεί έμφαση σε αρχές όπως ο περιορισμός του σκοπού ώστε να μην μπορεί να γίνει αδιάκριτη χρήση των δεδομένων, ιδιαίτερα των ειδικών κατηγοριών, που εισάγονται στο νέο σύστημα. Παράλληλα πρέπει να διασφαλιστούν προηγμένα τεχνολογικά συστήματα τα οποία θα διαχειρίζονται τα βιομετρικά δεδομένα και θα εξασφαλίζουν την ποιότητά τους. Επιπλέον πρέπει να δοθεί έμφαση στην αρχή της αναλογικότητας όσον αφορά και τις περιόδους διατήρησης των δεδομένων. Τέλος, η προστασία τους θα πρέπει να γίνει εκ του σχεδιασμού και να εξασφαλιστεί η ανιχνευσιμότητα και αποτελεσματική εποπτεία αυτών. Ειδικότερα σύμφωνα και με τις

προτάσεις του ΕΕΠΔ στα συμπεράσματα της γνωμοδότησης του (Ευρωπαϊός Επόπτης Προσωπικών Δεδομένων, 2017) είναι αναγκαία:

- Η ύπαρξη εκτίμησης επιπτώσεων όσον αφορά την προστασία των δεδομένων στα συστήματα πληροφοριών. Αν και κάτι τέτοιο προβλέπεται από τον ΓΚΠΔ, ωστόσο δεν έχει πραγματοποιηθεί στο πλαίσιο του SIS II. Η εκτίμηση επιπτώσεων είναι το κατάλληλο εργαλείο για την αξιολόγηση της αναγκαιότητας και της αναλογικότητας των αλλαγών που σχεδιάζονται, ειδικά ενώπιον της διεύρυνσης των κατηγοριών των δεδομένων που καταχωρίζονται και της επέκτασης αυτών στο πεδίο των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα.
- Αντιμετώπιση των ασαφειών σχετικά με την πρόσβαση στο σύστημα διαφόρων οργάνων και οργανισμών, οι οποίοι στα πλαίσια των καθηκόντων τους κάνουν αναζητήσεις και αντλούν δεδομένα από το SIS II. Είναι λοιπόν εξαιρετικά σημαντικό να είναι να υπάρχει ένα σαφές πλαίσιο σχετικά με τη λογοδοσία όλων των αρχών που έχουν πρόσβαση.
- Η έμφαση στη λογοδοσία μεταξύ του Ευρωπαϊκού Οργανισμού Συνοριοφυλακής Και Ακτοφυλακής και των κρατών μελών, ζητώντας τα κράτη-μέλη να θεωρούνται υπεύθυνοι επεξεργασίας δεδομένων σύμφωνα με το δίκαιο της Ένωσης σχετικά με τα προσωπικά δεδομένα και να αποσαφηνιστεί ότι αυτοί θα έχουν την τελική ευθύνη και λογοδοσία για την επεξεργασία των δεδομένων. Επίσης θεωρεί πως οι ομάδες της ευρωπαϊκής συνοριοφυλακής και ακτοφυλακής και όσοι συμμετέχουν στην εκτέλεση των καθηκόντων για την επιστροφή των υπηκόων τρίτων χωρών δεν θα πρέπει να έχουν πλήρη πρόσβαση σε όλες τις κατηγορίες καταχωρίσεων. Έτσι λοιπόν η αναφορά σχετικά με το ποιος θα πρέπει να έχει την πρόσβαση, θα πρέπει να είναι πολύ συγκεκριμένη και να περιορίζεται στους εκπροσώπους των εξουσιοδοτημένων φορέων.
- Η πρόβλεψη σχετικά με την υπέροχη ειδικών διατάξεων που βρίσκονται σε ισχύ ενώ στα πλαίσια της αρχής της νομιμότητας της επεξεργασίας που ανταποκρίνεται στο σκοπό για τον οποίο καταχωρίστηκε η πληροφορία, είναι θεμιτό να διευκρινιστεί υπό ποιες προϋποθέσεις μπορεί να αλλάξει ο σκοπός της επεξεργασίας αλλά και να δοθεί συγκεκριμένο περιεχόμενο στις έννοιες της δημόσιας τάξης και ασφάλειας ή της αποτροπής απειλής.

Η Ευρώπη μετά τις τρομοκρατικές επιθέσεις αλλά και την προσφυγική κρίση που βίωσε μία τελευταία χρόνια οδηγείται σε μεγαλύτερη εσωστρέφεια και διάθεση για διασφάλιση με κάθε μέσο της ασφάλειας στον ΧΕΑΔ. Αυτό φαίνεται στον τρόπο που

αντιμετώπισαν την προσφυγική κρίση αρκετά κράτη, κλείνοντας τα σύνορά τους και καταργώντας στην ουσία την ελεύθερη μετακίνηση στον ευρωπαϊκό χώρο, και υπό το φόβο της εισόδου τρομοκρατών ανάμεσα στους πρόσφυγες και μετανάστες. Η ενέργεια αυτή κατέδειξε στην ουσία το έλλειμμα ασφαλείας που βιώνουν και οι ευρωπαίοι. Αν και στους κανονισμούς προβλέπεται η προσωρινή αναστολή Σένγκεν, ωστόσο σε κάποιες από αυτές τις περιπτώσεις τα διαστήματα με κλειστά σύνορα υπερέβησαν τα επιτρεπόμενα χρονικά διαστήματα.

Πλέον στόχος της Ευρωπαϊκής Ένωσης είναι να διατηρήσει στην ουσία του το κεκτημένο Σένγκεν αυξάνοντας τα συστήματα πληροφοριών, αστυνόμευσης και επιβολής νόμου αλλά και εισάγοντας αυστηρότερους ελέγχους στα εξωτερικά της σύνορα. Ο ΧΕΑΔ ίσως κινδυνεύει έτσι να χάσει το χαρακτήρα της ελευθερίας και να μετατραπεί περισσότερο σε μία ζώνη αποκλεισμού, στο εσωτερικό της οποίας τίθενται σοβαροί προβληματισμοί σχετικά με τις επιπτώσεις της διαλειτουργικότητας όλων των συστημάτων στα δικαιώματα των ανθρώπων και στην προστασία των προσωπικών τους δεδομένων. Τα ζητήματα λοιπόν χρήζουν λεπτών χειρισμών και προσεκτικής εξέτασης κατά την διαμόρφωση της νομοθετικής βάσης των νέων συστημάτων, ώστε να ελαχιστοποιηθεί η πιθανότητα περιστολής δικαιωμάτων ή παραβίασης αυτών στο όνομα της ασφάλειας και να λειτουργήσει ο ευρωπαϊκός Χώρος Ελευθερίας Ασφαλείας και Δικαιοσύνης ως πραγματικό πεδίο ανάπτυξης των στόχων της Ευρωπαϊκής Ένωσης, προσφέροντας τα αδιαμφισβήτητα πλεονεκτήματά του σε όσους εισέρχονται σε αυτόν.

## Βιβλιογραφία

### Πρωτογενείς Πηγές

Κανονισμός Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 1725/2018/ΕΕ. *Για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ.* στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης: 21/11/2018, L 295/39

Ευρωπαίος Επόπτης Προσωπικών Δεδομένων, 2017. *Συνοπτική παρουσίαση της γνωμοδότησης του Ευρωπαϊκού Επόπτη Προστασίας Δεδομένων σχετικά με τη νέα νομική βάση του συστήματος πληροφοριών Σένγκεν.* στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης: 23/06/2017, C 200/14

Κανονισμός Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 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 για την Προστασία Δεδομένων).* στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης: 04/05/2016, L 348/131

Οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 2016/680/ΕΕ. *για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, διερεύνησης, ανίχνευσης ή δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της απόφασης-πλαίσιο 2008/977/ΔΕΥ του Συμβουλίου.* στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης: 04/05/2016, L 119/89

Απόφαση του Συμβουλίου 2008/976/ΔΕΥ. *σχετικά με το ευρωπαϊκό δικαστικό δίκτυο.* στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης: 24/12/2008, L 348/130

Απόφαση του Συμβουλίου 2007/533/ΔΕΥ. *σχετικά με την εγκατάσταση, τη λειτουργία και τη χρήση του συστήματος πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II).* στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης: 07/08/2007, L 205/63

Κανονισμός Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 2006/1987. *σχετικά με τη δημιουργία, τη λειτουργία και τη χρήση του Συστήματος Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II).* στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης: 28/12/2006, L 381/4

Κανονισμός Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου 2006/1986. *σχετικά με την πρόσβαση στο Σύστημα Πληροφοριών Σένγκεν δεύτερης γενιάς (SIS II) των υπηρεσιών των κρατών μελών που είναι υπεύθυνες για την έκδοση αδειών κυκλοφορίας οχημάτων.* στην Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης: 28/12/2006, L 381/1

Σύμβαση Εφαρμογής της Συμφωνίας Σένγκεν της 14<sup>ης</sup> Ιουνίου 1985, 2000. *μεταξύ των κυβερνήσεων των κρατών της Οικονομικής ένωσης Μπένελουξ, της Ομοσπονδιακής Δημοκρατίας της Γερμανίας και της Γαλλικής Δημοκρατίας, σχετικά με τη σταδιακή κατάργηση των ελέγχων στα σύνορα.* Στην Επίσημη Εφημερίδα των Κοινοτήτων: 22/09/2000

## Βιβλία

Οργανισμός Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης και Συμβούλιο της Ευρώπης, 2019. *Εγχειρίδιο Σχετικά με την Ευρωπαϊκή Νομοθεσία για την Προστασία Προσωπικών Δεδομένων.* Λουξεμβούργο: Υπηρεσία Εκδόσεων της Ευρωπαϊκής Ένωσης

Παπαγιάννης Δ., (2001). *Ο Ευρωπαϊκός Χώρος Ελευθερίας Ασφάλειας και Δικαιοσύνης.* Αθήνα – Κομοτηνή: Αντ. Ν. Σάκκουλας.

Παπαγιάννης Δ., (2008). *Ο χώρος της ασφάλειας στην Ευρωπαϊκή Ένωση.* Αθήνα – Κομοτηνή: Αντ. Ν. Σάκκουλας.

Τζώρτζη Β., (2018). *Προστασία Δεδομένων Προσωπικού Χαρακτήρα στον Χώρο ελευθερίας, Ασφάλειας και Δικαιοσύνης.* Αθήνα: Νομική Βιβλιοθήκη

Nugent, N., 2012. *Πολιτική και Διακυβέρνηση στην Ευρωπαϊκή Ένωση.* Αθήνα: Σαββάλλας.

Parkin J.,(2011). The difficult road to Schengen Information System II

## Ηλεκτρονικές Πηγές

Δικαστήριο της Ευρωπαϊκής Ένωσης, 2020. *Θεματικό Δελτίο: Προστασία Δεδομένων Προσωπικού Χαρακτήρα,* [Ηλεκτρονικό] Διαθέσιμο στο: [https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche\\_thematique\\_-\\_donnees\\_personnelles\\_-\\_el.pdf](https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_el.pdf)

Ευρωπαϊκή Ένωση, 2020. *Επίσημος ιστότοπος της Ευρωπαϊκής Ένωσης.* [Ηλεκτρονικό] Διαθέσιμο στο: [https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor\\_el](https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_el), [Τελευταία Πρόσβαση 02/09/2020]

Ευρωπαϊκή Ένωση, 2020α. *Ευρωπαϊκός Οργανισμός για τη Λειτουργική Διαχείριση Συστημάτων ΤΠ Μεγάλης Κλίμακας στον Χώρο Ελευθερίας.* [Ηλεκτρονικό] Διαθέσιμο στο: [https://europa.eu/european-union/about-eu/agencies/eu-lisa\\_el](https://europa.eu/european-union/about-eu/agencies/eu-lisa_el) [Τελευταία πρόσβαση 08/08/2020]

Ευρωπαϊκή Ένωση, 2020β. *Ευρωπαίος Επόπτης Προστασίας Δεδομένων (ΕΕΠΔ).* [Ηλεκτρονικό] Διαθέσιμο στο: [https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor\\_el](https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_el) [Τελευταία Πρόσβαση 08/08/2020]

Ευρωπαϊκό Κοινοβούλιο, 2020. *Σένγκεν: διεύρυνση της ζώνης ελεύθερης κυκλοφορίας της ΕΕ.* [Ηλεκτρονικό] Διαθέσιμο στο

<https://www.europarl.europa.eu/news/el/headlines/priorities/sengken-kai-europaika-sunora/20180216STO98008/sengken-dieurunsi-tis-zonis-eleutheris-kukloforias-tis-ee>  
[Τελευταία Πρόσβαση 04/08/2020]

Ευρωπαϊκό Κοινοβούλιο, 2020α. *Θεματολογικά Δελτία για την Ευρωπαϊκή Ένωση: Ελεύθερη Κυκλοφορία Προσώπων..* [Ηλεκτρονικό] Διαθέσιμο στο: <https://www.europarl.europa.eu/factsheets/el/sheet/147/vrij-verkeer-van-personen>,  
[Τελευταία πρόσβαση 4/08/2020].

Ευρωπαϊκό Κοινοβούλιο, 2020β. *Θεματολογικά Δελτία για την Ευρωπαϊκή Ένωση: Η Αρχή της Επικουρικότητας,* [Ηλεκτρονικό] Διαθέσιμο στο: [https://www.europarl.europa.eu/ftu/pdf/el/FTU\\_1.2.2.pdf](https://www.europarl.europa.eu/ftu/pdf/el/FTU_1.2.2.pdf) [Τελευταία πρόσβαση 04/08/2020].

Ευρωπαϊκό Κοινοβούλιο, 2018. *Revision of the Schengen Information System for border checks.* [Ηλεκτρονικό] Διαθέσιμο στο: [https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS\\_BRI%282017%29599341](https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI%282017%29599341) [Τελευταία πρόσβαση 09/08/2020].

Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2020. *Διωκτικές Αρχές – Ασφάλεια; Σχετικές Αποφάσεις της Αρχής.* [Ηλεκτρονικό] Διαθέσιμο στο [https://www.dpa.gr/portal/page?\\_pageid=33,126721&\\_dad=portal&\\_schema=PORTAL](https://www.dpa.gr/portal/page?_pageid=33,126721&_dad=portal&_schema=PORTAL)  
[Τελευταία Πρόσβαση 05/09/2020]

### Χρήσιμες Ιστοσελίδες

Ιστοσελίδα Αρχής προστασίας Δεδομένων Προσωπικού Χαρακτήρα, 2020. [www.dpa.gr](http://www.dpa.gr)  
[τελευταία πρόσβαση 14/09/2020]

Ιστοσελίδα Ευρωπαϊκής Ένωσης, 2020. [https://europa.eu/european-union/index\\_el](https://europa.eu/european-union/index_el)  
[τελευταία πρόσβαση 10/09/2020]

Ιστοσελίδα Ευρωπαϊκού Κοινοβουλίου, 2020 <https://www.europarl.europa.eu/portal/el>  
[τελευταία πρόσβαση 16/09/2020]

Ιστοσελίδα Ευρωπαϊού Επόπτη Προσωπικών Δεδομένων, 2020. [https://edps.europa.eu/edps-homepage\\_en?lang=el](https://edps.europa.eu/edps-homepage_en?lang=el) [τελευταία πρόσβαση 09/09/2020]

Ιστοσελίδα Δικαστηρίου της Ευρωπαϊκής Ένωσης, 2020. [https://curia.europa.eu/jcms/jcms/j\\_6/el/](https://curia.europa.eu/jcms/jcms/j_6/el/) [τελευταία πρόσβαση 16/09/2020]

Ιστοσελίδα Europol, 2020 <https://www.europol.europa.eu/el/about-europol> [τελευταία πρόσβαση 08/09/2020]



Ευρωπαϊκή Ένωση  
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης  
και Ευρωπαϊκό Ταμείο Συνοχής

Ε.Π.  
**ΜΕΤΑΡΡΥΘΜΙΣΗ  
ΔΗΜΟΣΙΟΥ  
ΤΟΜΕΑ**



ΕΣΠΑ  
2014-2020  
ανάπτυξη - εργασία - αλληλεγγύη

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Εθνική Σχολή Δημόσιας Διοίκησης και Αυτοδιοίκησης (ΕΣΔΔΑ)

Πειραιώς 211, ΤΚ 177 78, Ταύρος

τηλ: 2131306349 , fax: 2131306479

[www.ekdd.gr](http://www.ekdd.gr)