

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (679/2016/ΕΕ):

Μια πρώτη θεώρηση

Φερενίκης Παναγοπούλου

Επικουρη Καθηγήτρια Παντείου Πανεπιστημίου

Δ.Ν. (Humboldt), Μ.Δ.Ε. (Παν. Αθηνών), Μ.Ρ.Η. (Harvard)

I. Εισαγωγή

Στις 25 Μαΐου του 2018 ετέθη σε εφαρμογή ο Νέος Κανονισμός για την Προστασία Δεδομένων (679/2016/ΕΕ) με βασικό στόχο την ενίσχυση της προστασίας των προσωπικών δεδομένων των πολιτών. Η προγενέστερη Οδηγία (95/46/ΕΚ) -πρωτοποριακή για την εποχή της- ήταν λογικό μετά από μια εικοσαετία περίπου να ξεπεραστεί από την ιλιγγιώδη τεχνολογική ανάπτυξη.

Ο Νέος Κανονισμός λαμβάνει υπ' όψιν του τις νέες τεχνολογικές εφαρμογές θέτοντας ως ζητούμενο να συμβαδίζει το δίκαιο με την τεχνολογία και να μην την ακολουθεί ασθμαίνοντας. Είναι γεγονός ότι η εξέλιξη της τεχνολογίας έχει αλλάξει σε μεγάλο βαθμό την οικονομική και κοινωνική ζωή και πρέπει να διευκολύνει περαιτέρω την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ενώσεως και τη διαβίβαση σε τρίτες χώρες και διεθνείς οργανισμούς, διασφαλίζοντας παράλληλα υψηλό επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα (σκ. 7 Προοιμίου).

Δεν είναι τυχαία μάλιστα η επιλογή το τελικό κείμενο να λάβει το «ένδυμα» ενός Κανονισμού, που θα χαιρεί άμεσης και συνακόλουθα ομοιόμορφης και πιο εναρμονισμένης εφαρμογής από τα κράτη μέλη, και όχι μιας Οδηγίας, που θα απαιτεί την ενσωμάτωσή της από τα κράτη μέλη με νόμο. Ωστόσο, πρόκειται για έναν Κανονισμό με πολλά χαρακτηριστικά Οδηγίας, καθώς αναγνωρίζεται η διακριτική ευχέρεια στον εθνικό νομοθέτη για υιοθέτηση συγκεκριμένων επιλογών, π.χ. όσον αφορά στη χορήγηση αδειών επεξεργασίας ειδικών κατηγοριών δεδομένων (άρθρο 36 παρ. 5 Κ).

II. Προσωπικά δεδομένα ή ελεύθερη κυκλοφορία της πληροφορίας;

Ο Κανονισμός επισημαίνει emphatically στη σκέψη 4 του Προοιμίου ότι «το δικαίωμα προστασίας προσωπικών δεδομένων δεν είναι απόλυτο δικαίωμα· πρέπει να εκτιμάται σε σχέση με τη λειτουργία του στην κοινωνία και να σταθμίζεται με άλλα θεμελιώδη δικαιώματα, σύμφωνα με την αρχή της αναλογικότητας. Ο παρών κανονισμός σέβεται όλα τα θεμελιώδη δικαιώματα και τηρεί τις ελευθερίες και αρχές που αναγνωρίζονται στον Χάρτη όπως κατοχυρώνονται στις Συνθήκες, ιδίως τον σεβασμό της ιδιωτικής και οικογενειακής ζωής, της κατοικίας και των επικοινωνιών, την προστασία των δεδομένων προσωπικού χαρακτήρα, την ελευθερία σκέψης, συνείδησης και θρησκείας, την ελευθερία έκφρασης και πληροφόρησης, την επιχειρηματική ελευθερία, το δικαίωμα πραγματικής προσφυγής και αμερόληπτου δικαστηρίου και την πολιτιστική, θρησκευτική και γλωσσική πολυμορφία.» Παράλληλα, στο άρθρο 85 κατοχυρώνει την ελευθερία εκφράσεως και πληροφόρησης προβαίνοντας σε στάθμιση του δικαιώματος προστασίας δεδομένων προσωπικού χαρακτήρα με το δικαίωμα στην ελευθερία εκφράσεως και πληροφόρησης, συμπεριλαμβανομένης της επεξεργασίας για δημοσιογραφικούς σκοπούς. Υπό αυτή την

έννοια, τονίζεται ότι το δικαίωμα στην προστασία προσωπικών δεδομένων δεν είναι ένα απόλυτο και «τυραννικό» δικαίωμα.¹

Στην ουσία επαναλαμβάνεται, υπογραμμίζεται, αλλά και επικαιροποιείται η βασική αρχή της Οδηγίας 95/46/ΕΚ, η οποία θέτει επί ίσοις όροις ήδη στον τίτλο της την προστασία προσωπικών δεδομένων και την ελεύθερη διακίνηση των δεδομένων.² Εν τοις πράγμασι, η Οδηγία δεν αποσκοπούσε στην κατοχύρωση ενός απόλυτου δικαιώματος με απώτερο στόχο την προστασία της ιδιωτικής ζωής, αλλά στην απελευθέρωση της κυκλοφορίας δεδομένων εντός της Κοινότητας με τελικό στόχο τη μη παρεμπόδιση της ασκήσεως των τεσσάρων κοινοτικών ελευθεριών με όριο το θεμελιώδες δικαίωμα στην ιδιωτική ζωή.³ Επισημαίνεται, επίσης, ότι στη σχετική συζήτηση για την κατάρτιση της Οδηγίας υπερίσχυαν τα επιχειρήματα σχετικά με το οικονομικό σκέλος και την εσωτερική αγορά.⁴

Αυτό πρέπει να είναι και ένα μήνυμα για τον νέο Έλληνα νομοθέτη του υπό διαμόρφωση νόμου περί προστασίας προσωπικών δεδομένων, ο οποίος απαλλαγμένος από τον δίκαιο ενθουσιασμό και τον μαξιμαλισμό του νομοθέτη του ν. 2472/1997 πρέπει να εξισορροπήσει τα συγκρουόμενα συνταγματικά αγαθά, απεκδυόμενος του μαχητού τεκμηρίου «εν αμφιβολία υπέρ του υποκειμένου των δεδομένων» του ν. 2472/1997. Η επιλογή του Έλληνα νομοθέτη να εκφράσει την προτίμησή του στην προστασία δεδομένων προσωπικού χαρακτήρα, αφενός οδηγεί σε ασφάλεια δικαίου αναφορικά με το τι πρέπει να υπερισχύσει σε περίπτωση αμφιβολίας, αφετέρου, όμως, προκαλεί ερωτηματικά για το εάν θυσιάζεται η δικαιοσύνη της ατομικής περιπτώσεως μπροστά στην ασφάλεια δικαίου.⁵

III. Εννοιολογικές διασαφηνίσεις

Σύμφωνα με το άρθρο 4 ΓΚΠΔ «δεδομένα προσωπικού χαρακτήρα» είναι κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»): το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου». Η συνεισφορά του σχετικού ορισμού είναι ότι τα δεδομένα θέσεως (π.χ. στίγμα GPS) και τα επιγραμμικά δεδομένα χαρακτηρίζονται πλέον ρητά ως προσωπικά δεδομένα

Παράλληλα το άρθρο 9 ΓΚΠΔ κατατάσσει στην ειδική κατηγορία δεδομένων (αυτό που ο ν. 2472/1997 χαρακτήριζε ως ευαίσθητα δεδομένα) «τη φυλετική ή

¹ Βλ. *Χαράλαμπος Ανθόπουλος*, Προσωπικά δεδομένα και δικαιώματα, Εφημερίδα Έθνος, 18.1.2017, διαθέσιμο σε: http://www.ethnos.gr/xaralampos_anthopoulos/.

² Βλ. επίσης σκέψεις 3, 8 και 10 Προοιμίου της Οδηγίας 95/46/ΕΚ.

³ Βλ. *Βασιλική Ε. Χρήστου*, Το δικαίωμα στην προστασία από την επεξεργασία δεδομένων, Θεμελίωση-Ερμηνεία-Προοπτικές, Εκδόσεις Σάκκουλα, Αθήνα-Θεσσαλονίκη 2017, σ. 19 επ.

⁴ Βλ. Έγγραφο της Επιτροπής για την Προστασία των Ατόμων Σχετικά με την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα στην Κοινότητα και Ασφάλεια Πληροφοριών. COM (90) 314 final, 13 Σεπτεμβρίου 1990 και *Paul De Hert Serge Gutwirth*, Η προστασία δεδομένων προσωπικού χαρακτήρα στη νομολογία του Στρασβούργου και του Λουξεμβούργου: συνταγματοποίηση σε δράση, Μετάφραση-Επιμέλεια Ευάγγελου Παπακωνσταντίνου, ΕφημΔΔ 2010, σ. 57 επ. (61).

⁵ Βλ. *Φερενίκη Παναγοπούλου-Κουτνατζή*, Η λίστα Λαγκάρντ και τα όρια της ελευθερίας του τύπου, ΕφημΔΔ 2012, σ. 739 επ. (744 επ.).

εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό». Ο Κανονισμός πλέον εντάσσει ρητά στην ειδική κατηγορία δεδομένων τα βιομετρικά δεδομένα και τα γενετικά δεδομένα.

IV. Πεδίο εφαρμογής Κανονισμού

Σύμφωνα με το άρθρο 3 ΓΚΠΔ, το πεδίο εφαρμογής του Κανονισμού εκτείνεται στις δραστηριότητες εγκαταστάσεως υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία που λαμβάνει χώρα εντός ΕΕ, αλλά και στις δραστηριότητες εγκαταστάσεως υπευθύνου επεξεργασίας ή εκτελούντος την επεξεργασία εκτός ΕΕ όταν η επεξεργασία αφορά σε υποκείμενα δεδομένων που βρίσκονται εντός ΕΕ (π.χ. περιπτώσεις ηλεκτρονικού εμπορίου και καταρτίσεως προφίλ).

V. Νέα-ανανεωμένα δικαιώματα για τους πολίτες

1. Δικαίωμα στη λήθη: Σύμφωνα με το άρθρο 17 ΓΚΠΔ, κάθε ενδιαφερόμενος πολίτης μπορεί να ζητήσει από μηχανές αναζήτησεως να αφαιρέσουν συγκεκριμένα αποτελέσματα, εφόσον δεν θίγεται το δικαίωμα ενημερώσεως της κοινής γνώμης. Το μέχρι τούδε νομολογιακά διαμορφωμένο δικαίωμα συνίσταται στην απαλοιφή αποτελεσμάτων από τις μηχανές αναζήτησεως.⁶ Μεμονωμένα επίσης έχει αναγνωρισθεί δικαίωμα διαγραφής για διαδικτυακά αρχεία εφημερίδων.⁷ Καθοριστικής σημασίας είναι ο ρόλος των φορέων εκμεταλλεύσεως μηχανών αναζήτησεως, που με την ιδιότητα πλέον του υπευθύνου επεξεργασίας⁸ θα αξιολογούν το πρώτον τα αιτήματα διαγραφής υποκειμένων δεδομένων.

2. Ενίσχυση της παιδικής προστασίας: Οι γονείς πρέπει να συγκατατίθενται, σύμφωνα με το άρθρο 8 Κ, για τη συμμετοχή των παιδιών έως δεκαέξι ετών σε υπηρεσίες του διαδικτύου. Ο Κανονισμός αφήνει το περιθώριο στα κράτη μέλη να προβλέπουν δια νόμου μικρότερη ηλικία, όχι όμως κατώτερη των δεκατριών ετών. Αυτό που αξίζει προσοχής είναι η αναγνώριση της ευθύνης για τη λήψη της συγκαταθέσεως από τους

⁶ Βλ. ΔΕΕ, Απόφαση Google Spain SL, Google Inc. κατά Agencia Española de Protección de Datos, Mario Costeja González, 14.5.2014 στην υπόθεση C-131/12, έγγραφο εργασίας του WP225, 26-11-2014, διαθέσιμο σε: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf>, ΑΠΔΠΧ, Αποφάσεις 82, 83, 84/2016 και Πρακτικό της Συνεδριάσεως της Ολομέλειας της 28.6.2016.

⁷ Βλ. Tribunal Supremo, No 345/2015, 13.10.2015 (Ανώτατο Δικαστήριο Ισπανίας). Βλ. ανάλυση της αποφάσεως από Sebastian Schweda, Right to Be Forgotten, Also Applies to Online News Archive, Supreme Court Rules, European Data Protection Law Review 2015, σ. 301 επ. και Hanseatisches Oberlandesgericht Hamburg (Εφετείο του Αμβούργου), 7U 29/12, 7.7.2015, διαθέσιμο σε: <https://openjur.de/u/838786.html>. Βλ. ανάλυση της αποφάσεως από Sebastian Schweda, Hamburg Court of Appeal Obliges Pres Archive Operator to Prevent Name Search in Archived Articles, European Data Protection Law Review 2015, σ. 299 επ.

⁸ Βλ. Herke Kranenborg, όπ. ανωτ. (υποσ. **Error! Bookmark not defined.**), σ. 75-76.

ασκούντες τη γονική μέριμνα στον υπεύθυνο επεξεργασίας, ο οποίος οφείλει να καταβάλλει εύλογες προσπάθειες για να επαληθεύσει ότι η συγκατάθεση παρέχεται ή εγκρίνεται από το πρόσωπο που έχει τη γονική μέριμνα του παιδιού λαμβάνοντας υπ' όψιν τη διαθέσιμη τεχνολογία.

3. Δικαίωμα στη φορητότητα: Το σχετικό δικαίωμα συνίσταται, σύμφωνα με το άρθρο 20 Κ, στη δυνατότητα του υποκειμένου των δεδομένων, να λαμβάνει τα δεδομένα προσωπικού χαρακτήρα που το αφορούν και που έχει παράσχει σε υπεύθυνο επεξεργασίας, σε δομημένο, κοινώς χρησιμοποιούμενο και αναγνώσιμο από μηχανήματα διαλειτουργικό μορφότυπο, και να τα διαβιβάζει σε άλλον υπεύθυνο επεξεργασίας, όταν η επεξεργασία δεδομένων προσωπικού χαρακτήρα διενεργείται με αυτοματοποιημένα μέσα. Οι υπεύθυνοι επεξεργασίας των δεδομένων θα πρέπει να ενθαρρύνονται να αναπτύσσουν διαλειτουργικούς μορφότυπους που επιτρέπουν τη φορητότητα των δεδομένων.

4. Ενημέρωση σε περίπτωση παραβίασεως: Ο Κανονισμός επεκτείνει το υφιστάμενο δικαίωμα ενημερώσεως του υποκειμένου των δεδομένων στο πεδίο της ενημερώσεώς του από τον υπεύθυνο επεξεργασίας για την παραβίαση προσωπικών του δεδομένων τόσο στην εποπτική αρχή (άρθρο 33) όσο και στο υποκείμενο των δεδομένων (άρθρο 34). Όπως ορίζεται στη σκέψη 85 του Προοιμίου, οι υπεύθυνοι επεξεργασίας σε ορισμένες περιπτώσεις, πρέπει να κοινοποιούν τα περιστατικά παραβιάσεως δεδομένων προσωπικού χαρακτήρα εντός εβδομήντα δύο ωρών από την ανακάλυψη του περιστατικού παραβιάσεως και απώλειας προσωπικών δεδομένων στις αρμόδιες αρχές και στα υποκείμενα των δεδομένων αν η φύση των δεδομένων που χάθηκαν το απαιτεί. Εάν μια τέτοια γνωστοποίηση δεν μπορεί να επιτευχθεί εντός εβδομήντα δύο ωρών, η γνωστοποίηση θα πρέπει να συνοδεύεται από αιτιολογία η οποία αναφέρει τους λόγους της καθυστέρησης, οι πληροφορίες, δε, μπορούν να παρέχονται σταδιακά χωρίς αδικαιολόγητη καθυστέρηση.

5. Δικαίωμα στην ανθρώπινη παρέμβαση: Σύμφωνα με τη σκέψη 71 του Προοιμίου και το άρθρο 22 ΓΚΠΔ, το υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να μην υπόκειται σε απόφαση, με την οποία αξιολογούνται προσωπικές πτυχές που το αφορούν, και η οποία παράγει έννομα αποτελέσματα έναντι του προσώπου αυτού ή το επηρεάζει σημαντικά κατά ανάλογο τρόπο, λαμβανομένη αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας, όπως η αυτόματη άρνηση επιγραμμικής αιτήσεως πιστώσεως ή πρακτικές ηλεκτρονικών προσλήψεων χωρίς ανθρώπινη παρέμβαση.

6. Δικαίωμα περιορισμού της επεξεργασίας: Ένα επικαιροποιημένο δικαίωμα που κατοχυρώνεται στον Κανονισμό είναι το δικαίωμα περιορισμού της επεξεργασίας, κατά το άρθρο 18, υπό την έννοια της προσωρινής προστασίας του υποκειμένου των δεδομένων. Συγκεκριμένα, το υποκείμενο των δεδομένων δικαιούται να εξασφαλίζει από τον υπεύθυνο επεξεργασίας τον περιορισμό της επεξεργασίας, όταν α) η ακρίβεια των δεδομένων προσωπικού χαρακτήρα αμφισβητείται από το υποκείμενο των δεδομένων, για χρονικό διάστημα που επιτρέπει στον υπεύθυνο επεξεργασίας να επαληθεύσει την ακρίβεια των δεδομένων προσωπικού χαρακτήρα, β) η επεξεργασία είναι παράνομη και το υποκείμενο των δεδομένων αντιτάσσεται στη διαγραφή των δεδομένων προσωπικού χαρακτήρα και ζητεί, αντ' αυτής, τον περιορισμό της χρήσεως τους, γ) ο υπεύθυνος επεξεργασίας δεν χρειάζεται πλέον τα δεδομένα προσωπικού χαρακτήρα για τους σκοπούς της επεξεργασίας, αλλά τα δεδομένα αυτά απαιτούνται από το υποκείμενο των δεδομένων για τη θεμελίωση, την άσκηση ή την υποστήριξη νομικών αξιώσεων, δ) το υποκείμενο των δεδομένων έχει αντιρρήσεις για την επεξεργασία σύμφωνα με το άρθρο 21 παράγραφος 1, εν αναμονή της

επαληθεύσεως του κατά πόσον οι νόμιμοι λόγοι του υπευθύνου επεξεργασίας υπερσχύουν έναντι των λόγων του υποκειμένου των δεδομένων.

VII. Ενισχυμένες υποχρεώσεις προς τον Υπεύθυνο Επεξεργασίας

Η ενίσχυση των δικαιωμάτων των πολιτών επιτυγχάνεται μέσω της επιβολής ενισχυμένων υποχρεώσεων στους υπευθύνους επεξεργασίας. Η επαυξημένη ευθύνη του υπευθύνου επεξεργασίας συνιστά καινοτομία του Κανονισμού, καθώς το άρθρο 23 παρ. 2 της **Οδηγία 95/46/ΕΚ τον απαλλάσσει αν αποδείξει ότι δεν ευθύνεται** (άρθρο 23 Ν. 2472/97), ενώ ο Κανονισμός ορίζει ότι ο υπεύθυνος οφείλει να **εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα (ΚΤΟΜ) [& πολιτικές] για να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό [άρθρο 24§1]**

Οι υποχρεώσεις του υπευθύνου επεξεργασίας συνοψίζονται ακολούθως:

1. Κατάλληλα τεχνικά και οργανωτικά μέτρα: Ο υπεύθυνος επεξεργασίας οφείλει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει και να μπορεί να αποδεικνύει ότι η επεξεργασία διενεργείται σύμφωνα με τον Κανονισμό.

2. Δημιουργία κατά το σχεδιασμό (privacy by design) και εξ ορισμού κατάλληλης δομής (privacy by default): Ο υπεύθυνος επεξεργασίας οφείλει κατά το σχεδιασμό και εξ ορισμού να δημιουργήσει δομή, τεχνολογία και διαδικασίες που θα ανταποκρίνονται στις απαιτήσεις του Κανονισμού.

3. Υποχρέωση ενημερώσεως εποπτικής αρχής και υποκειμένου δεδομένων: Ο υπεύθυνος επεξεργασίας οφείλει να ενημερώσει την εποπτική αρχή και το υποκείμενο των δεδομένων αμελλητί από τη στιγμή που ενημερώθηκε για την παραβίαση δεδομένων. Τυχόν καταγγελία για παραβίαση συνιστά παράλληλα και ενημέρωσή του για την παραβίαση.

4. Κατάρτιση μελέτης εκτιμήσεως επιπτώσεων: Ο υπεύθυνος επεξεργασίας οφείλει να καταρτίσει μελέτη εκτιμήσεως αντικτύπου (impact assessment) για επεξεργασία δεδομένων που παρουσιάζουν υψηλό κίνδυνο και σχετίζονται με αξιολόγηση προσωπικών πτυχών, αφορούν σε δεδομένα μεγάλης κλίμακας ή σε παρακολούθηση δημοσίου χώρου.

5. Κατάρτιση πολιτικής ασφαλείας και κώδικων δεοντολογίας: Ο υπεύθυνος επεξεργασίας οφείλει να καταρτίζει πολιτικές ασφαλείας των δεδομένων και κώδικες δεοντολογίας.

6. Τήρηση αρχείων δραστηριοτήτων: Ο υπεύθυνος και εκτελών την επεξεργασία τηρούν εγγράφως ή ηλεκτρονικά αρχείο δραστηριοτήτων επεξεργασιών τους, όταν η επιχείρηση ή ο οργανισμός απασχολεί άνω των 250 ατόμων, η επεξεργασία δημιουργεί κινδύνους για τα δεδομένα, δεν είναι περιστασιακή ή περιλαμβάνει ειδικές κατηγορίες δεδομένων. Το εν λόγω αρχείο τίθεται στην διάθεση της εποπτικής Αρχής κατόπιν αιτήματος της προς άσκηση των αρμοδιοτήτων της.

5. Ορισμός Υπευθύνου Προστασίας Δεδομένων: Ο υπεύθυνος επεξεργασίας οφείλει να ορίσει υπεύθυνο προστασίας δεδομένων (data protection officer) σε περίπτωση που επεξεργάζεται δεδομένα μεγάλης κλίμακας.

VIII. Ο νέος θεσμός του υπευθύνου προστασίας δεδομένων

VIII. Περαιτέρω ζητήματα

1. Υπηρεσία μιας Στάσεως (One-Stop-Shop): Μια εταιρεία με θυγατρικές εταιρείες σε περισσότερα κράτη μέλη θα συνεργάζεται μόνο με την εποπτική αρχή του κράτους μέλους της κυρίας εγκατάστασης της επιχείρησής.

2. Υψηλά πρόστιμα: Επιβάλλονται πολύ υψηλά πρόστιμα που δύνανται να φτάσουν τα 20 εκατομμύρια Ευρώ ή το 4% του παγκόσμιου ετήσιου τζίρου μιας εταιρείας.

Η ευρύτερη προστασία των πολιτών είναι ένας από τους βασικούς στόχους του Κανονισμού, ο οποίος επιδιώκεται μέσω της ενισχύσεως των δικαιωμάτων των πολιτών και των αυξημένων υποχρεώσεων των εταιρειών. Για παράδειγμα, μέσω της υποχρεώσεως των εταιρειών να καταρτίζουν πολιτική ασφαλείας, κωδίκων δεοντολογίας και μελέτης εκτιμήσεως επιπτώσεων, ευαισθητοποιούνται εκ των πραγμάτων αναφορικά με την επεξεργασία των προσωπικών δεδομένων των πολιτών.

Ο Κανονισμός αποφορτίζει από τη μία πλευρά την Αρχή Προστασίας Δεδομένων από περιττά βάρη, όπως π.χ. τη λήψη γνωστοποιήσεως τηρήσεως αρχείου εκ μέρους του υπευθύνου επεξεργασίας, ενώ από την άλλη πλευρά της αναθέτει ουσιώδεις αρμοδιότητες. Όλες αυτές οι ενισχυμένες αρμοδιότητες των εποπτικών αρχών και ιδίως η απαίτηση για διενέργεια εκτιμήσεως αντίκτυπου, η προηγούμενη διαβούλευση με την Αρχή, η ενθάρρυνση της κατάρτισης κωδίκων δεοντολογίας και μηχανισμών πιστοποίησης σε συνδυασμό με την υποχρέωση διορισμού υπευθύνου προστασίας δεδομένων ενισχύουν τη συνεργασία μεταξύ υπευθύνων επεξεργασίας (λ.χ. ασφαλιστικών εταιρειών) και αρχών και κατ' αποτέλεσμα και την προστασία των δεδομένων.

Έτσι προτού η Αρχή καταλήξει στην επιβολή κάποιας κυρώσεως σε υπεύθυνο επεξεργασίας εταιρεία θα έχει προηγουμένως συνεργαστεί μαζί της καθώς επίσης και με τον υπεύθυνο προστασίας δεδομένων που έχει ορίσει παρέχοντας συμβουλευτική γνώμη, θα την έχει προειδοποιήσει και εάν παρόλη τη συνεργασία η εταιρεία δεν συμμορφωθεί στις υποδείξεις της Αρχής, αλλά και του υπευθύνου προστασίας δεδομένων, τότε θα υποστεί κυρώσεις.