ΕΚΤΕΛΕΣΤΙΚΗ ΑΠΟΦΑΣΗ (ΕΕ) 2021/1773 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 28ης Ιουνίου 2021

σύμφωνα με την οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με την επάρκεια της παρεχόμενης από το Ηνωμένο Βασίλειο προστασίας των δεδομένων προσωπικού χαρακτήρα

[κοινοποιηθείσα υπό τον αριθμό C(2021) 4801]

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη την οδηγία (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, 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 ([1]), και ιδίως το άρθρο 36 παράγραφος 3,

Εκτιμώντας τα ακόλουθα:

1. ΕΙΣΑΓΩΓΗ

(1) Η οδηγία (ΕΕ) 2016/680 θεσπίζει τους κανόνες που διέπουν τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές στην Ένωση προς τρίτες χώρες και διεθνείς οργανισμούς, εφόσον η εν λόγω διαβίβαση εμπίπτει στο πεδίο εφαρμογής της. Οι κανόνες για τις διεθνείς διαβιβάσεις δεδομένων από αρμόδιες αρχές καθορίζονται στο κεφάλαιο V της οδηγίας (ΕΕ) 2016/680, και ειδικότερα στα άρθρα 35 έως 40. Μολονότι η ροή δεδομένων προσωπικού χαρακτήρα προς και από χώρες εκτός της Ευρωπαϊκής Ένωσης είναι απαραίτητη για την αποτελεσματική συνεργασία στον τομέα της επιβολής του νόμου, θα πρέπει να διασφαλίζεται ότι το επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα στην Ευρωπαϊκή Ένωση δεν υπονομεύεται από τις διαβιβάσεις αυτές ([2]).

(2) Σύμφωνα με το άρθρο 36 παράγραφος 3 της οδηγίας (ΕΕ) 2016/680, η Επιτροπή μπορεί να αποφασίσει, μέσω εκτελεστικής πράξης, ότι εξασφαλίζεται επαρκές επίπεδο προστασίας από τρίτη χώρα, έδαφος ή έναν ή περισσότερους συγκεκριμένους τομείς σε τρίτη χώρα ή από διεθνή οργανισμό. Υπό την προϋπόθεση αυτή, οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα μπορούν να πραγματοποιούνται χωρίς να απαιτείται περαιτέρω έγκριση (εκτός εάν χρειάζεται να δώσει την έγκρισή του για τη διαβίβαση άλλο κράτος μέλος από το οποίο παρελήφθησαν τα δεδομένα), όπως προβλέπεται στο άρθρο 35 παράγραφος 1 και στην αιτιολογική σκέψη 66 της οδηγίας (ΕΕ) 2016/680.

(3) Όπως ορίζεται στο άρθρο 36 παράγραφος 2 της οδηγίας (ΕΕ) 2016/680, για την έκδοση απόφασης περί επάρκειας απαιτείται διεξοδική ανάλυση της έννομης τάξης της τρίτης χώρας. Στην εκτίμησή της, η Επιτροπή πρέπει να προσδιορίζει αν η εν λόγω τρίτη χώρα εγγυάται επίπεδο προστασίας «κατ' ουσίαν ισοδύναμο» μ' αυτό που προβλέπει η Ευρωπαϊκή Ένωση [αιτιολογική σκέψη 67 της οδηγίας (ΕΕ) 2016/680]. Το πρότυπο με βάση το οποίο αξιολογείται η «κατ' ουσίαν ισοδυναμία» είναι εκείνο που καθορίζεται από τη νομοθεσία της ΕΕ, ειδικότερα από την οδηγία (ΕΕ) 2016/680, καθώς και από τη νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης ([3]). Σημαντικά από την άποψη αυτή είναι επίσης τα σημεία αναφοράς για την επάρκεια του Ευρωπαϊκού Συμβουλίου Προστασίας Δεδομένων ([4]).

(4) Όπως έχει διευκρινιστεί από το Δικαστήριο της Ευρωπαϊκής Ένωσης, αυτό δεν συνεπάγεται απαίτηση για ίδιο ακριβώς επίπεδο προστασίας ([5]). Ειδικότερα, τα μέσα που χρησιμοποιεί η τρίτη χώρα για την προστασία των δεδομένων προσωπικού χαρακτήρα μπορούν να διαφέρουν από αυτά που εφαρμόζονται εντός της Ευρωπαϊκής Ένωσης, εφόσον αποδεικνύονται στην πράξη αποτελεσματικά ώστε να διασφαλίζουν επαρκές επίπεδο προστασίας ([6]). Συνεπώς, το κριτήριο της επάρκειας δεν επιβάλλει πιστή αντιγραφή των κανόνων της Ένωσης. Το καθοριστικό στοιχείο είναι κυρίως αν, μέσω της ουσίας των δικαιωμάτων περί προστασίας της ιδιωτικής ζωής, της αποτελεσματικής εφαρμογής τους, καθώς και της δυνατότητας επιβολής και εποπτείας τους, το σύστημα της τρίτης χώρας ως σύνολο προσφέρει το απαιτούμενο επίπεδο προστασίας ([7]).

([1]) ΕΕ L 119 της 4.5.2016, σ. 89.

([2]) Βλέπε αιτιολογική σκέψη 64 της οδηγίας (ΕΕ) 2016/680.

([3]) Βλέπε, πιο πρόσφατα, υπόθεση C-311/18, Maximilian Schrems κατά Data Protection Commissioner (στο εξής: Schrems II) ECLI:EU:C:2020:559.

([4]) Βλέπε Συστάσεις 01/2021 σχετικά με τα σημεία αναφοράς για την επάρκεια στο πλαίσιο της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, οι οποίες εκδόθηκαν τον Φεβρουάριο του 2021 και διατίθενται στον ακόλουθο σύνδεσμο https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines-recommendations-best-practices_el

([5]) Υπόθεση C-362/14, Maximilian Schrems κατά Data Protection Commissioner (στο εξής: Schrems), ECLI:EU:C:2015:650, σκέψη 73.

([6]) Schrems, σκέψη 74.

([7]) Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο, Ανταλλαγή και προστασία των δεδομένων προσωπικού χαρακτήρα σε έναν παγκοσμιοποιημένο κόσμο, COM(2017) 7 της 10.1.2017, ενότητα 3.1, σ. 6-7, διατίθεται στον ακόλουθο σύνδεσμο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:52017DC0007&from=EN.

(5) Η Επιτροπή έχει αναλύσει προσεκτικά τη σχετική νομοθεσία και την πρακτική του Ηνωμένου Βασιλείου. Με βάση τα πορίσματά της, όπως αναφέρονται κατωτέρω, η Επιτροπή καταλήγει στο συμπέρασμα ότι το Ηνωμένο Βασίλειο διασφαλίζει επαρκές επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται από αρμόδιες αρχές στην Ένωση, οι οποίες εμπίπτουν στο πεδίο εφαρμογής της οδηγίας (ΕΕ) 2016/680, σε αρμόδιες αρχές του Ηνωμένου Βασιλείου που εμπίπτουν στο πεδίο εφαρμογής του μέρους 3 του νόμου του 2018 για την προστασία των δεδομένων (Data Protection Act 2018 – DPA 2018) ([8]).

(6) Η παρούσα απόφαση έχει ως αποτέλεσμα οι εν λόγω διαβιβάσεις να μπορούν να πραγματοποιούνται χωρίς να απαιτείται περαιτέρω έγκριση για περίοδο τεσσάρων ετών, η οποία υπόκειται σε πιθανή ανανέωση, και με την επιφύλαξη των προϋποθέσεων που ορίζονται στο άρθρο 35 της οδηγίας (ΕΕ) 2016/680.

2. ΚΑΝΟΝΕΣ ΠΟΥ ΕΦΑΡΜΟΖΟΝΤΑΙ ΣΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΑΠΟ ΑΡΜΟΔΙΕΣ ΑΡΧΕΣ ΓΙΑ ΤΟΥΣ ΣΚΟΠΟΥΣ ΤΗΣ ΕΠΙΒΟΛΗΣ ΤΟΥ ΠΟΙΝΙΚΟΥ ΔΙΚΑΙΟΥ

2.1. Το συνταγματικό πλαίσιο

(7) Το πολίτευμα του Ηνωμένου Βασιλείου είναι κοινοβουλευτική δημοκρατία. Διαθέτει κυρίαρχο κοινοβούλιο, το οποίο είναι ανώτερο όλων των άλλων κρατικών οργάνων, εκτελεστική εξουσία η οποία προέρχεται από το κοινοβούλιο και λογοδοτεί σ' αυτό, και ανεξάρτητη δικαστική εξουσία. Η εκτελεστική εξουσία αντλεί την εξουσία της από την ικανότητά της να διαχειρίζεται την εμπιστοσύνη της εκλεγμένης Βουλής των Κοινοτήτων και λογοδοτεί σε αμφότερα τα σώματα του Κοινοβουλίου [Βουλή των Κοινοτήτων (House of Commons) και Βουλή των Λόρδων (House of Lords)] που είναι αρμόδια για τον έλεγχο της κυβέρνησης και για τη συζήτηση και ψήφιση των νόμων. Το κοινοβούλιο του Ηνωμένου Βασιλείου έχει εκχωρήσει αρμοδιότητες στο Κοινοβούλιο της Σκωτίας, στο Κοινοβούλιο της Ουαλίας (Senedd Cymru) και στη Συνέλευση της Βόρειας Ιρλανδίας για τη θέσπιση νομοθεσίας σχετικά με ορισμένα εσωτερικά ζητήματα της Σκωτίας, της Ουαλίας και της Βόρειας Ιρλανδίας. Παρότι η προστασία των δεδομένων αποτελεί θέμα που εμπίπτει στην αποκλειστική αρμοδιότητα του Κοινοβουλίου του Ηνωμένου Βασιλείου, δηλαδή η ίδια νομοθεσία ισχύει σε ολόκληρη τη χώρα, άλλοι τομείς πολιτικής που σχετίζονται με την παρούσα απόφαση έχουν αποκεντρωθεί. Για παράδειγμα, τα συστήματα ποινικής δικαιοσύνης, συμπεριλαμβανομένης της αστυνόμευσης (δηλαδή των δραστηριοτήτων που ασκούνται από τις αστυνομικές δυνάμεις) της Σκωτίας και της Βόρειας Ιρλανδίας έχουν αποκεντρωθεί στο Κοινοβούλιο της Σκωτίας και στη Συνέλευση της Βόρειας Ιρλανδίας, αντίστοιχα ([9]).

(8) Παρότι το Ηνωμένο Βασίλειο δεν διαθέτει κωδικοποιημένο σύνταγμα υπό την έννοια ενός παγιωμένου συνταγματικού εγγράφου, οι συνταγματικές του αρχές έχουν προκύψει με την πάροδο του χρόνου από τη νομολογία και από συμβάσεις. Έχει αναγνωριστεί η συνταγματική αξία ορισμένων νόμων, όπως η Magna Carta, η Διακήρυξη των Δικαιωμάτων του 1689 (Bill of Rights 1689) και ο νόμος του 1998 για τα ανθρώπινα δικαιώματα (Human Rights Act 1998). Τα θεμελιώδη δικαιώματα των προσώπων έχουν αναπτυχθεί, ως μέρος του συντάγματος, μέσω του κοινοδικαίου, των νόμων και διεθνών συνθηκών, ειδικότερα μέσω της Ευρωπαϊκής σύμβασης Δικαιωμάτων του Ανθρώπου (ΕΣΔΑ), την οποία το Ηνωμένο Βασίλειο κύρωσε το 1951. Το Ηνωμένο Βασίλειο κύρωσε επίσης τη σύμβαση του Συμβουλίου της Ευρώπης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα (σύμβαση 108) το 1987 ([10]).

(9) Ο νόμος του 1998 για τα ανθρώπινα δικαιώματα ενσωματώνει, στο δίκαιο του Ηνωμένου Βασιλείου, τα δικαιώματα που περιέχονται στην ΕΣΔΑ. Ο εν λόγω νόμος παρέχει σε κάθε πρόσωπο τα θεμελιώδη δικαιώματα και τις ελευθερίες που κατοχυρώνονται στα άρθρα 2 έως 12 και στο άρθρο 14 της ΕΣΔΑ και στα άρθρα 1 έως 3 του πρώτου πρωτοκόλλου της, καθώς και στο άρθρο 1 του δέκατου τρίτου πρωτοκόλλου της, σε συνδυασμό με τα άρθρα 16 έως 18 της ΕΣΔΑ. Μεταξύ αυτών περιλαμβάνεται το δικαίωμα στον σεβασμό της ιδιωτικής και οικογενειακής ζωής, το οποίο με τη σειρά του περιλαμβάνει το δικαίωμα στην προστασία των δεδομένων και το δικαίωμα στη χρηστή απονομή δικαιοσύνης ([11]). Συγκεκριμένα, σύμφωνα με το άρθρο 8 της ΕΣΔΑ, δεν επιτρέπεται να υπάρξει επέμβαση δημόσιας αρχής κατά την άσκηση του δικαιώματος στην ιδιωτική ζωή, εκτός εάν η επέμβαση αυτή προβλέπεται από τον νόμο και αποτελεί μέτρο το οποίο, σε μια δημοκρατική κοινωνία, είναι αναγκαίο για την εθνική ασφάλεια, τη δημόσια ασφάλεια, την οικονομική ευημερία της χώρας, την προάσπιση της τάξης και την πρόληψη ποινικών παραβάσεων, την προστασία της υγείας ή της ηθικής, ή την προστασία των δικαιωμάτων και ελευθεριών άλλων.

([8]) Ο νόμος του 2018 για την προστασία των δεδομένων διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2018/12/contents

([9]) UK Explanatory Framework for Adequacy Discussions, section F: Law enforcement, διατίθεται στον ακόλουθο σύνδεσμο: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

([10]) Οι αρχές της σύμβασης 108 μεταφέρθηκαν αρχικά στο δίκαιο του Ηνωμένου Βασιλείου μέσω του νόμου του 1984 για την προστασία των δεδομένων, ο οποίος αντικαταστάθηκε από τον DPA 1998 και στη συνέχεια από τον DPA 2018 [σε συνδυασμό με τον γενικό κανονισμό προστασίας δεδομένων (ΓΚΠΔ) του Ηνωμένου Βασιλείου]. Το Ηνωμένο Βασίλειο υπέγραψε επίσης το πρωτόκολλο για την τροποποίηση της σύμβασης για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία πληροφοριών προσωπικού χαρακτήρα (γνωστή ως «Σύμβαση 108+») το 2018 και επί του παρόντος βρίσκεται σε διαδικασία κύρωσης της εν λόγω σύμβασης.

([11]) Άρθρα 6 και 8 της ΕΣΔΑ (βλέπε επίσης παράρτημα 1 του νόμου του 1998 για τα ανθρώπινα δικαιώματα).

(10) Σύμφωνα με τον νόμο του 1998 για τα ανθρώπινα δικαιώματα, οποιαδήποτε ενέργεια των δημόσιων αρχών πρέπει να είναι συμβατή με δικαίωμα που κατοχυρώνεται από την ΕΣΔΑ ([12]). Επιπλέον, η πρωτογενής και η παράγωγη νομοθεσία πρέπει να ερμηνεύονται και να εφαρμόζονται με τρόπο που συνάδει με τα δικαιώματα αυτά ([13]). Εφόσον ένα πρόσωπο θεωρεί ότι τα δικαιώματά του, συμπεριλαμβανομένων των δικαιωμάτων στην προστασία της ιδιωτικής ζωής και των δεδομένων, έχουν παραβιαστεί από δημόσιες αρχές, μπορεί να ζητήσει έννομη προστασία προσφεύγοντας ενώπιον των δικαστηρίων του Ηνωμένου Βασιλείου βάσει του νόμου του 1998 για τα ανθρώπινα δικαιώματα και εντέλει, αφού εξαντλήσει τα εθνικά ένδικα βοηθήματα και μέσα, να ζητήσει έννομη προστασία ενώπιον του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου για παραβιάσεις των δικαιωμάτων που κατοχυρώνονται στην ΕΣΔΑ.

2.2. **Το πλαίσιο για την προστασία των δεδομένων στο Ηνωμένο Βασίλειο**

(11) Το Ηνωμένο Βασίλειο αποχώρησε από την Ευρωπαϊκή Ένωση στις 31 Ιανουαρίου 2020. Βάσει της συμφωνίας για την αποχώρηση του Ηνωμένου Βασιλείου της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας από την Ευρωπαϊκή Ένωση και την Ευρωπαϊκή Κοινότητα Ατομικής Ενέργειας ([14]), το ενωσιακό δίκαιο συνέχισε να εφαρμόζεται στο Ηνωμένο Βασίλειο κατά τη μεταβατική περίοδο έως τις 31 Ιανουαρίου 2020. Πριν από την αποχώρηση και κατά τη διάρκεια της μεταβατικής περιόδου, το νομοθετικό πλαίσιο για την προστασία των δεδομένων προσωπικού χαρακτήρα στο Ηνωμένο Βασίλειο που διέπει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους, απαρτιζόταν από τα σχετικά μέρη του νόμου του 2018 για την προστασία των δεδομένων, με τον οποίο μεταφέρθηκε στο εθνικό δίκαιο η οδηγία (ΕΕ) 2016/680.

(12) Για να προετοιμαστεί για την αποχώρηση από την ΕΕ, η κυβέρνηση του Ηνωμένου Βασιλείου θέσπισε τον νόμο του 2018 για την αποχώρηση από την Ευρωπαϊκή Ένωση [European Union (Withdrawal) Act – EUWA] ([15]), στον οποίο ενσωματώνεται η άμεσα εφαρμοστέα νομοθεσία της Ένωσης στο δίκαιο του Ηνωμένου Βασιλείου και προβλέπεται ότι η λεγόμενη «εσωτερική νομοθεσία που προέρχεται από την ΕΕ» εξακολουθεί να παράγει αποτελέσματα μετά τη λήξη της μεταβατικής περιόδου. Το μέρος 3 του DPA 2018 ([16]) για τη μεταφορά της οδηγίας (ΕΕ) 2016/680 στο εθνικό δίκαιο αποτελεί «εσωτερική νομοθεσία που προέρχεται από την ΕΕ» στο πλαίσιο του νόμου του 2018 για την αποχώρηση από την Ευρωπαϊκή Ένωση. Σύμφωνα με τον νόμο του 2018 για την αποχώρηση από την Ευρωπαϊκή Ένωση, η μη τροποποιημένη «εσωτερική νομοθεσία που προέρχεται από την ΕΕ» πρέπει να ερμηνεύεται από τα δικαστήρια του Ηνωμένου Βασιλείου σύμφωνα με τη σχετική νομολογία του Δικαστηρίου της Ευρωπαϊκής Ένωσης (στο εξής: Δικαστήριο) και τις γενικές αρχές του δικαίου της Ένωσης όπως ίσχυαν αμέσως πριν από τη λήξη της μεταβατικής περιόδου (στο εξής: «διατηρούμενη νομολογία της ΕΕ» και «διατηρούμενες γενικές αρχές του δικαίου της ΕΕ», αντίστοιχα) ([17]).

(13) Βάσει του νόμου του 2018 για την αποχώρηση από την Ευρωπαϊκή Ένωση, οι υπουργοί του Ηνωμένου Βασιλείου έχουν την εξουσία να θεσπίζουν παράγωγο δίκαιο, μέσω νομοθετικών πράξεων, ώστε να επιφέρουν τις αναγκαίες τροποποιήσεις στη διατηρούμενη νομοθεσία της ΕΕ ως συνέπεια της αποχώρησης του Ηνωμένου Βασιλείου από την Ένωση. Η εξουσία αυτή ασκήθηκε μέσω των κανονισμών του 2019 για την προστασία των δεδομένων, την ιδιωτική ζωή και τις ηλεκτρονικές επικοινωνίες (τροποποιήσεις κ.λπ.) (αποχώρηση από την ΕΕ) (κανονισμοί DPPEC) ([18]). Οι κανονισμοί αυτοί τροποποιούν τη νομοθεσία του Ηνωμένου Βασιλείου για την προστασία των δεδομένων, συμπεριλαμβανομένου του DPA 2018, ώστε να ανταποκρίνεται στο εθνικό πλαίσιο ([19]).

([12]) Άρθρο 6 του νόμου του 1998 για τα ανθρώπινα δικαιώματα.

([13]) Άρθρο 3 του νόμου του 1998 για τα ανθρώπινα δικαιώματα.

([14]) Συμφωνία για την αποχώρηση του Ηνωμένου Βασιλείου της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας από την Ευρωπαϊκή Ένωση και την Ευρωπαϊκή Κοινότητα Ατομικής Ενέργειας (2019/C 384 I/01, XT/21054/2019/INIT, ΕΕ C 384I της 12.11.2019, σ. 1) (στο εξής: συμφωνία αποχώρησης), διατίθεται στον ακόλουθο σύνδεσμο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN.

([15]) Νόμος του 2018 για την αποχώρηση από την Ευρωπαϊκή Ένωση, διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2018/16/contents

([16]) Ο νόμος του 2018 για την προστασία των δεδομένων διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2018/12/contents

([17]) Άρθρο 6 του νόμου του 2018 για την αποχώρηση από την Ευρωπαϊκή Ένωση.

([18]) The Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019, διατίθενται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/uksi/2019/419/contents/made, όπως τροποποιήθηκαν με τους κανονισμούς DPPEC 2020, οι οποίοι διατίθενται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([19]) Οι κανονισμοί για την αποχώρηση από την ΕΕ επιφέρουν σειρά τροποποιήσεων στο μέρος 3 του DPA 2018. Πολλές από αυτές είναι τροποποιήσεις τεχνικής φύσης, όπως η διαγραφή των αναφορών σε «κράτος μέλος» ή στην «οδηγία για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου» [βλέπε για παράδειγμα, άρθρο 48 παράγραφος 8 ή άρθρο 73 παράγραφος 5 στοιχείο α) του DPA 2018 με το «εσωτερικό δίκαιο»], ώστε το μέρος 3 να λειτουργεί ουσιαστικά ως εσωτερικό δίκαιο μετά τη λήξη της μεταβατικής περιόδου. Σε ορισμένα σημεία απαιτήθηκαν άλλα είδη αλλαγών, για παράδειγμα, όσον αφορά το «ποιος» εκδίδει «αποφάσεις περί επάρκειας» για τους σκοπούς του νομοθετικού πλαισίου του Ηνωμένου Βασιλείου για την προστασία των δεδομένων (βλέπε άρθρο 74A του DPA 2018), δηλαδή ο ανώτερος υπουργός (Secretary of State) αντί της Ευρωπαϊκής Επιτροπής.

(14) Κατά συνέπεια, τα νομικά πρότυπα για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές για τους σκοπούς της πρόληψης, της διερεύνησης, της ανίχνευσης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους στο Ηνωμένο Βασίλειο μετά τη μεταβατική περίοδο βάσει της συμφωνίας αποχώρησης θα εξακολουθήσουν να καθορίζονται στα σχετικά μέρη του DPA 2018, όπως όμως τροποποιήθηκαν με τους κανονισμούς DPPEC, ειδικότερα στο μέρος 3 του εν λόγω νόμου. Ο γενικός κανονισμός του Ηνωμένου Βασιλείου για την προστασία των δεδομένων (στο εξής: ΓΚΠΔ του Ηνωμένου Βασιλείου) δεν εφαρμόζεται σ' αυτό το είδος επεξεργασίας.

(15) Στο μέρος 3 του DPA 2018 προβλέπονται οι κανόνες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς επιβολής του ποινικού δικαίου, συμπεριλαμβανομένων των αρχών προστασίας των δεδομένων, των νόμιμων λόγων επεξεργασίας (νομιμότητα), των δικαιωμάτων των υποκειμένων των δεδομένων, των υποχρεώσεων των αρμόδιων αρχών ως υπευθύνων επεξεργασίας και των περιορισμών στις περαιτέρω διαβιβάσεις. Ταυτόχρονα, οι εφαρμοστέοι κανόνες σχετικά με την εποπτεία, την επιβολή και την έννομη προστασία που εφαρμόζονται στον τομέα της επιβολής του νόμου προβλέπονται στα μέρη 5 και 6 του DPA 2018.

(16) Επιπλέον, δεδομένου του σχετικού ρόλου που διαδραματίζουν οι αστυνομικές δυνάμεις στον τομέα της επιβολής του νόμου, θα πρέπει να ληφθούν υπόψη οι κανόνες που διέπουν την αστυνόμευση. Καθώς η αστυνόμευση αποτελεί αποκεντρωμένο ζήτημα, υπάρχουν διάφορες νομοθετικές πράξεις, οι οποίες ωστόσο είναι συχνά παρόμοιες ως προς το περιεχόμενό τους, που εφαρμόζονται στον τομέα της αστυνόμευσης α) στην Αγγλία και την Ουαλία, β) στη Σκωτία και γ) στη Βόρεια Ιρλανδία ([20]). Επιπλέον, υπάρχουν διάφορα είδη εγγράφων καθοδήγησης που παρέχουν πρόσθετες διευκρινίσεις σχετικά με τον τρόπο με τον οποίο θα πρέπει να ασκούνται οι εξουσίες της αστυνομίας. Υπάρχουν τρεις βασικές μορφές καθοδήγησης της αστυνομίας: 1) θεσμοθετημένη καθοδήγηση που εκδίδεται βάσει νομοθεσίας, όπως ο κώδικας δεοντολογίας ([21]) και ο κώδικας ορθής πρακτικής για τη διαχείριση πληροφοριών της αστυνομίας (κώδικας ορθής πρακτικής MoPI) ([22]) ο οποίος έχει εκδοθεί βάσει του νόμου του 1996 για την αστυνομία (Police Act 1996) ([23]) ή οι κώδικες PACE ([24]) που έχουν εκδοθεί στο πλαίσιο του νόμου για την αστυνομία και τα αποδεικτικά στοιχεία σε ποινικές διαδικασίες (Police and Criminal Evidence Act) ([25]), 2) εγκεκριμένη επαγγελματική πρακτική για τη διαχείριση πληροφοριών της αστυνομίας (APP Guidance on the Management of Police Information) ([26]), η οποία έχει εκδοθεί από το Σώμα των Εργαζομένων στην Αστυνόμευση (College of Policing) και 3) επιχειρησιακές οδηγίες (οι οποίες δημοσιεύονται από την ίδια την αστυνομία). Το Εθνικό Συμβούλιο Αρχηγών της Αστυνομίας (National Police Chiefs Council) (συντονιστικό όργανο για το σύνολο των αστυνομικών δυνάμεων του Ηνωμένου Βασιλείου) δημοσιεύει επιχειρησιακές οδηγίες τις οποίες έχουν υιοθετήσει όλες οι αστυνομικές δυνάμεις και οι οποίες εφαρμόζονται, ως εκ τούτου, σε εθνικό επίπεδο ([27]). Σκοπός αυτής της καθοδήγησης είναι να διασφαλίσει τη συνέπεια μεταξύ των δυνάμεων όσον αφορά τον τρόπο διαχείρισης των πληροφοριών ([28]).

(17) Ο κώδικας ορθής πρακτικής MoPI εκδόθηκε από τον ανώτερο υπουργό το 2005, με χρήση των εξουσιών που προβλέπονται στο άρθρο 39Α του νόμου του 1996 για την αστυνομία ([29]). Κάθε κώδικας ορθής πρακτικής που εκδίδεται δυνάμει του νόμου για την αστυνομία πρέπει να έχει την έγκριση του ανώτερου υπουργού και υπόκειται σε διαβούλευση με την Εθνική Υπηρεσία Δίωξης του Εγκλήματος (National Crime Agency, NCA) πριν υποβληθεί στο Κοινοβούλιο. Βάσει του άρθρου 39Α παράγραφος 7 του νόμου για την αστυνομία, η αστυνομία είναι υποχρεωμένη να λαμβάνει δεόντως υπόψη

([20]) Για λεπτομερέστερη επεξήγηση σχετικά με τις αστυνομικές δυνάμεις και τις εξουσίες τους στο Ηνωμένο Βασίλειο, βλέπε: UK Explanatory Framework for Adequacy Discussions, section F: Law Enforcement (βλέπε υποσημείωση 9).

([21]) Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales, διατίθεται στον ακόλουθο σύνδεσμο: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf· Police Service Northern Ireland Code of Ethics, διατίθεται στον ακόλουθο σύνδεσμο: https://www.nipolicingboard.org.uk/psni-code-ethics· Code of Ethics for policing in Scotland, διατίθεται στον ακόλουθο σύνδεσμο: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/.

([22]) Code of Practice on the Management of Police Information, διατίθεται στον ακόλουθο σύνδεσμο: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf.

([23]) Νόμος του 1996 για την αστυνομία, διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/1996/16/contents.

([24]) Κώδικες ορθής πρακτικής βάσει του νόμου του 1984 για την αστυνομία και τα αποδεικτικά στοιχεία σε ποινικές διαδικασίες (PACE), διατίθενται στον ακόλουθο σύνδεσμο: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) Νόμος του 1984 για την αστυνομία και τα αποδεικτικά στοιχεία σε ποινικές διαδικασίες, διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/1984/60/contents.

([26]) Authorised Professional Practice on the Management of Police Information, διατίθεται στον ακόλουθο σύνδεσμο: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/.

([27]) Data Protection Manual for Police Data Protection Professionals, διατίθεται στον ακόλουθο σύνδεσμο: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf.

([28]) Για παράδειγμα, ο κώδικας ορθής πρακτικής MoPI (βλέπε υποσημείωση 22) εφαρμόζεται στη διατήρηση επιχειρησιακών πληροφοριών αστυνόμευσης (βλέπε αιτιολογική σκέψη (47) της παρούσας απόφασης).

([29]) Σύμφωνα με τις πληροφορίες που παρασχέθηκαν από τις αρχές του Ηνωμένου Βασιλείου, κατά την περίοδο των συνομιλιών σχετικά με την επάρκεια, το Σώμα των Εργαζομένων στην Αστυνόμευση (College of Policing) βρισκόταν σε διαδικασία κατάρτισης κώδικα ορθής πρακτικής για τη διαχείριση πληροφοριών και αρχείων προς αντικατάσταση του MoPI. Το σχέδιο κώδικα δημοσιεύτηκε για δημόσια διαβούλευση στις 25 Ιανουαρίου 2021 και διατίθεται στον ακόλουθο σύνδεσμο: https://www.college.police.uk/article/information-records-management-consultation

τους κώδικες που εκδίδονται δυνάμει του συγκεκριμένου νόμου, και ως εκ τούτου, αναμένεται να συμμορφώνεται μ' αυτόν ([30]). Επιπλέον, η μη θεσμοθετημένη καθοδήγηση [όπως το έγγραφο καθοδήγησης εγκεκριμένης επαγγελματικής πρακτικής (APP) για τη διαχείριση πληροφοριών της αστυνομίας] πρέπει να συνάδει πάντοτε με τον κώδικα ορθής πρακτικής MoPI ο οποίος υπερισχύει ([31]). Σε κάθε περίπτωση, παρότι ενδέχεται να υπάρχουν ορισμένες επιχειρησιακές καταστάσεις στις οποίες χρειάζεται οι αστυνομικοί να παρεκκλίνουν από αυτή την καθοδήγηση, υποχρεούνται παρ' όλα αυτά να συμμορφώνονται με τις απαιτήσεις του μέρους 3 του DPA 2018 ([32]).

(18) Περαιτέρω καθοδήγηση σχετικά με τη νομοθεσία για την προστασία των δεδομένων στο Ηνωμένο Βασίλειο όσον αφορά την επεξεργασία στον τομέα της επιβολής του νόμου παρέχεται από τον Επίτροπο Πληροφοριών [στο εξής: «Επίτροπος Πληροφοριών» (Information Commissioner) ή «Γραφείο Επιτρόπου Πληροφοριών» (Information Commissioner's Office, ICO)] ([33]) (για περισσότερες λεπτομέρειες σχετικά με το ICO, βλέπε αιτιολογικές σκέψεις (93) έως (109)). Παρότι ο σχετικός οδηγός δεν είναι νομικά δεσμευτικός, σε μια δικαστική υπόθεση, τα δικαστήρια θα πρέπει να λαμβάνουν υπόψη τυχόν παράβασή του, καθώς έχει ερμηνευτική βαρύτητα και καταδεικνύει τον τρόπο με τον οποίο ερμηνεύεται και εφαρμόζεται η νομοθεσία από τον Επίτροπο στην πράξη ([34]).

(19) Τέλος, όπως αναφέρεται στις αιτιολογικές σκέψεις (8) έως (10), οι υπηρεσίες επιβολής του νόμου του Ηνωμένου Βασιλείου πρέπει να διασφαλίζουν τη συμμόρφωση με την ΕΣΔΑ και τη σύμβαση 108.

(20) Ως εκ τούτου, όσον αφορά τη δομή και τις κύριες συνιστώσες του, το νομικό πλαίσιο που διέπει την επεξεργασία δεδομένων από τις αρχές επιβολής του ποινικού δικαίου στο Ηνωμένο Βασίλειο, είναι σε μεγάλο βαθμό παρόμοιο με εκείνο που ισχύει στην ΕΕ. Στις ομοιότητες περιλαμβάνεται το γεγονός ότι το εν λόγω πλαίσιο δεν βασίζεται μόνο σε υποχρεώσεις που προβλέπονται στο εθνικό δίκαιο, το οποίο έχει διαμορφωθεί από το δίκαιο της ΕΕ, αλλά και σε υποχρεώσεις που κατοχυρώνονται στο διεθνές δίκαιο, ιδίως μέσω της προσχώρησης του Ηνωμένου Βασιλείου στην ΕΣΔΑ και στη σύμβαση 108, καθώς και μέσω της υπαγωγής του στη δικαιοδοσία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου. Οι υποχρεώσεις αυτές που απορρέουν από νομικά δεσμευτικές διεθνείς πράξεις, κυρίως όσον αφορά την προστασία των δεδομένων προσωπικού χαρακτήρα, αποτελούν, ως εκ τούτου, ιδιαίτερα σημαντικό στοιχείο του νομικού πλαισίου που αξιολογείται στην παρούσα απόφαση.

2.3. **Καθ' ύλην και εδαφικό πεδίο εφαρμογής**

(21) Το καθ' ύλην πεδίο εφαρμογής του μέρους 3 του DPA 2018 συμπίπτει με το πεδίο εφαρμογής της οδηγίας 2016/680, όπως προσδιορίζεται στο άρθρο 2 παράγραφος 2 αυτής. Το μέρος 3 εφαρμόζεται στην αυτοματοποιημένη, εν όλω ή εν μέρει, επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδια αρχή, καθώς και στη μη αυτοματοποιημένη επεξεργασία, από αρμόδια αρχή, δεδομένων προσωπικού χαρακτήρα που περιλαμβάνονται ή πρόκειται να περιληφθούν σε αρχείο.

(22) Επιπλέον, προκειμένου να εμπίπτει στο πεδίο εφαρμογής του εν λόγω μέρους 3, ο υπεύθυνος επεξεργασίας πρέπει να είναι «αρμόδια αρχή» και η επεξεργασία πρέπει να διενεργείται για «σκοπό επιβολής του νόμου». Ως εκ τούτου, το καθεστώς προστασίας δεδομένων που αξιολογείται στην παρούσα απόφαση εφαρμόζεται σε όλες τις δραστηριότητες επιβολής του νόμου των εν λόγω αρμόδιων αρχών.

(23) Η έννοια της «αρμόδιας αρχής» ορίζεται στο άρθρο 30 του DPA ως πρόσωπο που περιλαμβάνεται στο παράρτημα 7 του DPA 2018, καθώς και ως οποιοδήποτε άλλο πρόσωπο στον βαθμό που το εν λόγω πρόσωπο έχει εκ του νόμου καθήκοντα για οποιονδήποτε από τους σκοπούς επιβολής του νόμου. Οι αρμόδιες αρχές που παρατίθενται στο παράρτημα 7 δεν περιλαμβάνουν μόνο αστυνομικές δυνάμεις, αλλά και όλες τις υπουργικές κρατικές υπηρεσίες, καθώς και άλλες αρχές με

([30]) Στην υπόθεση R κατά Commission of Police of the Metropolis [2014] EWCA Civ 585, επιβεβαιώθηκε το νομικό καθεστώς του κώδικα ορθής πρακτικής MoPI και ο δικαστής Λόρδος Laws δήλωσε ότι ο Διοικητικής της Μητροπολιτικής Αστυνομίας του Λονδίνου είναι υποχρεωμένος να λαμβάνει υπόψη τον κώδικα ορθής πρακτικής MoPI και το έγγραφο καθοδήγησης εγκεκριμένης επαγγελματικής πρακτικής (APP) για τη διαχείριση πληροφοριών της αστυνομίας, σύμφωνα με το άρθρο 39A του νόμου του 1996 για την αστυνομία.

([31]) Η αστυνομία επιθεωρείται ως προς τη συμμόρφωσή της με τον κώδικα ορθής πρακτικής MoPI από την επιθεώρηση αστυνομικών, πυροσβεστικών και διασωστικών υπηρεσιών του Ηνωμένου Βασιλείου (Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services, HMICFRS).

([32]) Βλέπε σχετικά, τη θέση του Σώματος των Εργαζομένων στην Αστυνόμευση σχετικά με τη συμμόρφωση με την καθοδήγηση APP για όλα τα στοιχεία αστυνόμευσης, στην οποία εξηγείται ότι η APP είναι εγκεκριμένη από τον επαγγελματικό φορέα αστυνόμευσης (το Σώμα των Εργαζομένων στην Αστυνόμευση) ως επίσημη πηγή επαγγελματικής πρακτικής στον τομέα της αστυνόμευσης. Οι αστυνομικοί και το προσωπικό οφείλουν να λαμβάνουν υπόψη την APP κατά την άσκηση των καθηκόντων τους. Ωστόσο, υπάρχουν ορισμένες περιπτώσεις στις οποίες υπάρχει θεμιτός επιχειρησιακός λόγος για παρέκκλιση μιας δύναμης από την APP, υπό την προϋπόθεση ότι υπάρχει σαφές σκεπτικό γι' αυτή την ενέργεια. Η οικεία δύναμη φέρει την ευθύνη για κάθε τοπικό και εθνικό κίνδυνο που απορρέει από τη λειτουργία εκτός του πλαισίου των εθνικά συμφωνημένων κατευθυντήριων γραμμών και, εάν προκύψει κατά συνέπεια κάποιο περιστατικό ή έρευνα (όπως π.χ. μέσω της Ανεξάρτητης Υπηρεσίας Δεοντολογίας της Αστυνομίας), η δύναμη είναι υπεύθυνη για κάθε κίνδυνο». Διατίθεται στον ακόλουθο σύνδεσμο https://www.app.college.police.uk/faq-page/.

([33]) Guide to Law Enforcement Processing, διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

([34]) Βλέπε υπόθεση Bridges κατά Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) όπου, μολονότι επισημάνθηκε ο μη θεσμοθετημένος χαρακτήρας της καθοδήγησης που εκδίδει ο Επίτροπος, το Ανώτερο Δικαστήριο (High Court) ανέφερε ότι «προκειμένου να εξετάσει αν ένας υπεύθυνος επεξεργασίας έχει συμμορφωθεί με την υποχρέωση του άρθρου 64 [διεξαγωγή εκτίμησης επιπτώσεων σχετικά με την προστασία των δεδομένων σε περίπτωση επεξεργασίας υψηλού κινδύνου], το δικαστήριο λαμβάνει υπόψη τον οδηγό που έχει εκδώσει ο Επίτροπος Πληροφοριών όσον αφορά τις εκτιμήσεις επιπτώσεων σχετικά με την προστασία των δεδομένων».

ερευνητικά καθήκοντα [π.χ. ο Επίτροπος της Φορολογικής και Τελωνειακής Αρχής του Ηνωμένου Βασιλείου (Commissioner for Her Majesty's Revenue and Customs), η Αρχή Εσόδων της Ουαλίας (Welsh Revenue Authority), η Αρχή Ανταγωνισμού και Αγορών (Competition and Markets Authority) ή το Κτηματολόγιο του Ηνωμένου Βασιλείου (Her Majesty's Land Register) ή η Εθνική Υπηρεσία Δίωξης του Εγκλήματος], εισαγγελικές υπηρεσίες, άλλες υπηρεσίες ποινικής δικαιοσύνης και άλλοι κάτοχοι αξιωμάτων ή φορείς που ασκούν δραστηριότητες επιβολής του νόμου ([35]). Το μέρος 3 του DPA 2018 εφαρμόζεται επίσης στα δικαστήρια και στα δικαιοδοτικά όργανα όταν ασκούν τα δικαστικά τους καθήκοντα, με εξαίρεση το μέρος που αφορά τα δικαιώματα του υποκειμένου των δεδομένων και την εποπτεία του ICO ([36]). Ο κατάλογος των αρμόδιων αρχών που παρατίθεται στο παράρτημα 7 δεν είναι οριστικός και μπορεί να επικαιροποιείται από τον ανώτερο υπουργό με κανονισμούς λαμβανομένων υπόψη των αλλαγών στην οργάνωση των δημόσιων αξιωμάτων ([37]).

(24) Η εν λόγω επεξεργασία πρέπει επίσης να έχει «σκοπό επιβολής του νόμου», ο οποίος ορίζεται ως η πρόληψη, διερεύνηση, ανίχνευση ή δίωξη ποινικών αδικημάτων ή η εκτέλεση ποινικών κυρώσεων, περιλαμβανομένων της προστασίας από απειλές κατά της δημόσιας ασφάλειας και της αποτροπής τους ([38]). Η επεξεργασία από αρμόδια αρχή δεν διέπεται από το μέρος 3 του DPA 2018, όταν δεν πραγματοποιείται για σκοπούς επιβολής του νόμου. Αυτό ισχύει, για παράδειγμα, στην περίπτωση που η Αρχή Ανταγωνισμού και Αγορών ερευνά υποθέσεις που δεν έχουν ποινικοποιηθεί (π.χ. συγχωνεύσεις μεταξύ εταιρειών). Στην περίπτωση αυτή, εφαρμόζεται ο ΓΚΠΔ του Ηνωμένου Βασιλείου, μαζί με το μέρος 2 του DPA 2018, καθώς η επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις αρμόδιες αρχές πραγματοποιείται για άλλους σκοπούς, και όχι για σκοπούς επιβολής του νόμου. Προκειμένου να καθοριστεί ποιο καθεστώς προστασίας δεδομένων εφαρμόζεται (μέρος 3 ή μέρος 2 του DPA 2018) στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, η αρμόδια αρχή, δηλαδή ο υπεύθυνος επεξεργασίας, πρέπει να εξετάσει αν ο «πρωταρχικός σκοπός» της εν λόγω επεξεργασίας είναι ένας από τους σκοπούς επιβολής του νόμου που προβλέπονται στον DPA 2018.

(25) Όσον αφορά το εδαφικό πεδίο εφαρμογής του μέρους 3 του DPA 2018, το άρθρο 207 παράγραφος 2 προβλέπει ότι ο DPA εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των δραστηριοτήτων προσώπου που διαθέτει εγκατάσταση σε ολόκληρο το έδαφος του Ηνωμένου Βασιλείου. Μεταξύ αυτών περιλαμβάνονται οι δημόσιες αρχές των εδαφών της Αγγλίας, της Ουαλίας, της Σκωτίας και της Βόρειας Ιρλανδίας οι οποίες εμπίπτουν στο καθ' ύλην πεδίο εφαρμογής του μέρους 3 του DPA 2018 ([39]).

2.3.1. *Ορισμός των δεδομένων προσωπικού χαρακτήρα και της επεξεργασίας*

(26) Οι βασικές έννοιες των δεδομένων προσωπικού χαρακτήρα και της επεξεργασίας ορίζονται στο άρθρο 3 του DPA 2018 και εφαρμόζονται σε ολόκληρη την έκταση του εν λόγω νόμου. Οι ορισμοί ακολουθούν πιστά τους αντίστοιχους ορισμούς που παρατίθενται στο άρθρο 3 της οδηγίας 2016/680. Βάσει του DPA 2018, ως δεδομένα προσωπικού χαρακτήρα νοείται κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο εν ζωή πρόσωπο ([40]). Σύμφωνα με το άρθρο 3 παράγραφος 3 του DPA 2018, ένα πρόσωπο είναι ταυτοποιήσιμο εάν η ταυτότητά του μπορεί να εξακριβωθεί άμεσα ή έμμεσα από τις πληροφορίες, μεταξύ άλλων μέσω αναφοράς σε όνομα ή αναγνωριστικό στοιχείο ταυτότητας ή μέσω αναφοράς σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του προσώπου. Η έννοια της «επεξεργασίας» ορίζεται ως πράξη ή σειρά πράξεων που πραγματοποιείται σε πληροφορίες ή σε σύνολα πληροφοριών, όπως α) η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση ή η αποθήκευση· β) η προσαρμογή ή η μεταβολή· γ) η ανάκτηση, η αναζήτηση πληροφοριών ή η χρήση· δ) η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης· ε) η συσχέτιση ή ο συνδυασμός· ή στ) ο περιορισμός, η διαγραφή ή η καταστροφή. Επιπλέον, στον νόμο ορίζεται η «επεξεργασία ευαίσθητων δεδομένων» ως «α) η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση· β) η επεξεργασία γενετικών δεδομένων ή βιομετρικών δεδομένων, με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου· γ) η επεξεργασία δεδομένων που αφορούν την υγεία· δ) η επεξεργασία δεδομένων που αφορούν τη σεξουαλική ζωή ή τον γενετήσιο προσανατολισμό ενός προσώπου» ([41]). Στο πλαίσιο αυτό, στο άρθρο 205 του DPA 2018 παρατίθεται ο ορισμός των «βιομετρικών δεδομένων» ([42]), των «δεδομένων που αφορούν την υγεία» ([43]) και των «γενετικών δεδομένων» ([44]).

([35]) Μεταξύ αυτών, το παράρτημα 7 του DPA 2018 περιλαμβάνει τους διευθυντές εισαγγελικών αρχών, τον διευθυντή εισαγγελικών αρχών της Βόρειας Ιρλανδίας ή τον Επίτροπο Πληροφοριών.

([36]) Άρθρο 43 παράγραφος 3 του DPA 2018.

([37]) Άρθρο 30 παράγραφος 3 του DPA 2018. Οι υπηρεσίες πληροφοριών [Μυστική Υπηρεσία Πληροφοριών (Secret Intelligence Service), Υπηρεσία Ασφάλειας (Security Service) και Κεντρική Κυβερνητική Υπηρεσία Επικοινωνιών (Government Communications Headquarters)] δεν αποτελούν αρμόδιες αρχές (βλέπε άρθρο 30 παράγραφος 2 του DPA 2018), επομένως το μέρος 3 του DPA 2018 δεν εφαρμόζεται σε καμία από τις δραστηριότητές τους. Οι δραστηριότητές τους εμπίπτουν στο πεδίο εφαρμογής του μέρους 4 του DPA 2018.

([38]) Άρθρο 31 του DPA 2018.

([39]) Αυτό σημαίνει ότι ο DPA 2018 και, ως εκ τούτου, η παρούσα απόφαση δεν εφαρμόζονται στις εξαρτήσεις του Στέμματος του Ηνωμένου Βασιλείου και στα λοιπά υπερπόντια εδάφη του Ηνωμένου Βασιλείου, όπως για παράδειγμα οι Νήσοι Φόκλαντ και το έδαφος του Γιβραλτάρ.

([40]) Τα δεδομένα προσωπικού χαρακτήρα που αφορούν αποθανόν πρόσωπο δεν εμπίπτουν στο πεδίο εφαρμογής του DPA 2018.

([41]) Άρθρο 35 παράγραφος 8 του DPA 2018.

([42]) «Βιομετρικά δεδομένα»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα.

([43]) «Δεδομένα που αφορούν την υγεία»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του.

([44]) «Γενετικά δεδομένα»: δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με τη φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου.

(27) Το άρθρο 32 του DPA 2018 αποσαφηνίζει τους ορισμένους του «υπεύθυνου επεξεργασίας» και του «εκτελούντος την επεξεργασία» στο πλαίσιο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα για σκοπούς επιβολής του νόμου, ακολουθώντας πιστά τους αντίστοιχους ορισμούς της οδηγίας 2016/680. Ο υπεύθυνος επεξεργασίας είναι η αρμόδια αρχή που καθορίζει τους σκοπούς και τα μέσα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Όταν η επεξεργασία απαιτείται από τον νόμο, ο υπεύθυνος επεξεργασίας είναι η αρμόδια αρχή στην οποία επιβάλλεται η υποχρέωση αυτή από τον εν λόγω νόμο. Ο εκτελών την επεξεργασία ορίζεται ως κάθε πρόσωπο που επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας (εκτός από πρόσωπο που είναι υπάλληλος του υπευθύνου επεξεργασίας).

2.4. **Εγγυήσεις, δικαιώματα και υποχρεώσεις**

2.4.1. *Νομιμότητα και αντικειμενικότητα της επεξεργασίας*

(28) Σύμφωνα με το άρθρο 35 του DPA 2018, η επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να είναι σύννομη και δίκαιη, κατά τρόπο παρόμοιο με το άρθρο 4 παράγραφος 1 στοιχείο α) της οδηγίας (ΕΕ) 2016/680. Σύμφωνα με το άρθρο 35 παράγραφος 2 του DPA 2018, η επεξεργασία δεδομένων προσωπικού χαρακτήρα για οποιονδήποτε από τους σκοπούς επιβολής του νόμου είναι σύννομη μόνον εφόσον βασίζεται στο δίκαιο και είτε το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία για τον σκοπό αυτόν, είτε η επεξεργασία είναι αναγκαία για την εκτέλεση καθήκοντος που ασκείται για τον σκοπό αυτόν από αρμόδια αρχή.

2.4.1.1. Επεξεργασία βάσει του δικαίου

(29) Όπως ορίζεται και στο άρθρο 8 της οδηγίας (ΕΕ) 2016/680, προκειμένου να διασφαλίζεται η νομιμότητα της επεξεργασίας που εμπίπτει στο μέρος 3 του DPA 2018, η εν λόγω επεξεργασία πρέπει να «βασίζεται στο δίκαιο». «Σύννομη» είναι η επεξεργασία που επιτρέπεται είτε εκ του νόμου είτε βάσει του κοινοδικαίου είτε βάσει βασιλικών προνομίων ([45]).

(30) Οι εξουσίες των αρμόδιων αρχών διέπονται κατά κανόνα από νόμους, που σημαίνει ότι τα καθήκοντα και οι εξουσίες τους καθορίζονται σαφώς σε νομοθετικές πράξεις που εγκρίνονται από το Κοινοβούλιο ([46]). Σε ορισμένες περιπτώσεις, η αστυνομία, καθώς και άλλες αρμόδιες αρχές που παρατίθενται στο παράρτημα 7 του DPA 2018 μπορούν να βασίζονται στο κοινοδίκαιο για την επεξεργασία δεδομένων ([47]). Το κοινοδίκαιο έχει οικοδομηθεί μέσω των προηγουμένων που θέτουν οι αποφάσεις των δικαστηρίων. Το κοινοδίκαιο έχει σημασία στο πλαίσιο των εξουσιών που διαθέτει η αστυνομία η οποία αντλεί από τη συγκεκριμένη πηγή δικαίου το βασικό της καθήκον να προστατεύει το κοινό μέσω της ανίχνευσης και της πρόληψης των εγκλημάτων ([48]). Ωστόσο, οι αστυνομικές δυνάμεις διαθέτουν εξουσίες που απορρέουν τόσο από το κοινοδίκαιο όσο και από

([45]) Επεξηγηματικές σημειώσεις του DPA 2018, παράγραφος 181, διατίθενται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpgaen_20180012_en.pdf.

([46]) Η Εθνική Υπηρεσία Δίωξης του Εγκλήματος, για παράδειγμα, αντλεί τις εξουσίες της από τον νόμο του 2013 για τη δίωξη του εγκλήματος και τα δικαστήρια (Crime and Courts Act 2013), ο οποίος διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2013/22/contents. Αντίστοιχα, οι εξουσίες της Υπηρεσίας Τυποποίησης Τροφίμων προβλέπονται από τον νόμο του 1999 για την τυποποίηση τροφίμων, ο οποίος διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/1999/28/contents. Άλλα παραδείγματα περιλαμβάνουν τον νόμο του 1985 για τη δίωξη των παραβατών (Prosecution of Offenders Act 1985), με τον οποίο δημιουργήθηκε η Εισαγγελική Αρχή του Στέμματος (Crown Prosecution Service) (βλέπε https://www.legislation.gov.uk/ukpga/1985/23/contents)· τον νόμο του 2005 για τους Επιτρόπους της Φορολογικής και Τελωνειακής Αρχής (Commissioners for Revenue and Customs Act 2005), με τον οποίο συστάθηκε η Φορολογική και Τελωνειακή Αρχή του Ηνωμένου Βασιλείου (Her Majesty's Revenue and Customs) (βλέπε https://www.legislation.gov.uk/ukpga/2005/11/contents)· τον νόμο του 1995 για την ποινική δικονομία (Σκωτία) [Criminal Procedure (Scotland) Act 1995], με τον οποίο συστάθηκε η Επιτροπή Ελέγχου Ποινικών Υποθέσεων της Σκωτίας (Scottish Criminal Cases Review Commission) (βλέπε https://www.legislation.gov.uk/ukpga/1995/46/contents)· τον νόμο του 2002 για τη δικαιοσύνη (Βόρεια Ιρλανδία) [Justice (Northern Ireland) Act 2002], με τον οποίο ιδρύθηκε η Εισαγγελική Αρχή (Public Prosecution Service, PPS) της Βόρειας Ιρλανδίας (βλέπε https://www.legislation.gov.uk/ukpga/2002/26/contents) και δημιουργήθηκε η υπηρεσία σοβαρών περιπτώσεων απάτης (Serious Fraud Office), η οποία έλαβε τις εξουσίες της δυνάμει του νόμου του 1987 για την ποινική δικαιοσύνη (Criminal Justice Act 1987) (βλέπε https://www.legislation.gov.uk/ukpga/1987/38/contents).

([47]) Για παράδειγμα, σύμφωνα με τις πληροφορίες που παρασχέθηκαν από τις αρχές του Ηνωμένου Βασιλείου, στο πλαίσιο της Εισαγγελίας της Σκωτίας (Crown Office and Procurator Fiscal Service), η οποία είναι αρμόδια για τη δίωξη υποθέσεων στη Σκωτία, ο Γενικός Εισαγγελέας (Lord Advocate), ο οποίος είναι επικεφαλής του συστήματος δίωξης στη Σκωτία, αντλεί τις εξουσίες του για τη διερεύνηση θανάτων και τη δίωξη αδικημάτων από το κοινοδίκαιο, ενώ κάποια από τα καθήκοντά του ορίζονται βάσει νόμου. Επιπλέον, το Στέμμα, και κατ' επέκταση διάφορα υπουργεία και υπουργοί της κυβέρνησης, αντλούν επίσης τις εξουσίες τους από έναν συνδυασμό νομοθεσίας, κοινοδικαίου και βασιλικού προνομίου (πρόκειται για εξουσίες βάσει του κοινοδικαίου που ανατίθενται στο Στέμμα αλλά ασκούνται από υπουργούς).

([48]) UK Explanatory Framework for Adequacy Discussions, section F: Law Enforcement, σ. 8 (βλέπε υποσημείωση 9).

νομοθετικές πράξεις ([49]) για την εκτέλεση αυτού του καθήκοντος. Όταν η αστυνομία διαθέτει εξουσία εκ του νόμου, αυτή υπερισχύει έναντι κάθε εξουσίας που απορρέει από το κοινοδίκαιο ([50]).

(31) Έχει αναγνωριστεί από τα δικαστήρια ότι το εύρος των εξουσιών και υποχρεώσεων του αστυνομικού, όπως απορρέουν από το κοινοδίκαιο, περιλαμβάνει «όλα τα μέτρα που θεωρεί αναγκαία για τη διατήρηση της ειρήνης, την πρόληψη του εγκλήματος ή την προστασία της περιουσίας από ζημία λόγω εγκληματικής πράξης» ([51]). Οι εξουσίες που απορρέουν από το κοινοδίκαιο δεν είναι ανεπιφύλακτες. Υπόκεινται σε σειρά περιορισμών, συμπεριλαμβανομένων των ορίων που έχουν καθοριστεί από τα δικαστήρια ([52]) και από τη νομοθεσία, και ειδικότερα από τον νόμο του 1998 για τα ανθρώπινα δικαιώματα και τον νόμο του 2010 για την ισότητα (Equality Act 2010) ([53]). Επιπλέον, για τις αρμόδιες αρχές που επεξεργάζονται δεδομένα βάσει του μέρους 3 του DPA 2018, στο πλαίσιο αυτό περιλαμβάνεται και η άσκηση των εξουσιών που απορρέουν από το κοινοδίκαιο σύμφωνα με τις απαιτήσεις που ορίζονται στον DPA 2018 ([54]). Επίσης, κάθε απόφαση για την εκτέλεση κάθε είδους επεξεργασίας δεδομένων πρέπει να λαμβάνει υπόψη τις απαιτήσεις των εφαρμοστέων οδηγιών, όπως ο κώδικας ορθής πρακτικής MoPI, καθώς και τις ειδικές οδηγίες για μία από τις χώρες του Ηνωμένου Βασιλείου ([55]). Η κυβέρνηση και η επιχειρησιακή αστυνομία εκδίδουν σειρά εγγράφων καθοδήγησης για να διασφαλίσουν ότι οι αστυνομικοί ασκούν τις αρμοδιότητές τους εντός των ορίων που θέτει το κοινοδίκαιο ή ο σχετικός νόμος ([56]).

(32) Τα βασιλικά προνόμια αποτελούν μια άλλη συνιστώσα του «δικαίου» και αναφέρονται σε ορισμένες εξουσίες που έχουν ανατεθεί στο Στέμμα και μπορούν να ασκούνται από την εκτελεστική εξουσία και τα οποία δεν βασίζονται στον νόμο, αλλά απορρέουν από την κυριαρχία του μονάρχη ([57]). Υπάρχουν ελάχιστα παραδείγματα εξουσιών που απορρέουν από τα βασιλικά προνόμια και είναι συναφή στο πλαίσιο της επιβολής του νόμου. Περιλαμβάνουν, για παράδειγμα, το πλαίσιο αμοιβαίας δικαστικής συνδρομής που επιτρέπει την κοινοποίηση δεδομένων από ανώτερο υπουργό σε τρίτες χώρες για

([49]) Οι βασικές νομοθετικές πράξεις που προβλέπουν το καθεστώς σχετικά με τις κύριες αστυνομικές εξουσίες (σύλληψη, έρευνες, έγκριση συνέχισης της κράτησης, λήψη δακτυλικών αποτυπωμάτων, λήψη προσωπικών δειγμάτων, εντολές παρακολούθησης, πρόσβαση σε δεδομένα επικοινωνίας) είναι οι εξής: i) για την Αγγλία και την Ουαλία, ο νόμος του 1984 για την αστυνομία και τα αποδεικτικά στοιχεία σε ποινικές διαδικασίες (PACE), ο οποίος διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/1984/60/contents, όπως τροποποιήθηκε με τον νόμο του 2012 για την προστασία των ελευθεριών (Protection of Freedoms Act 2012, PoFA), ο οποίος διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2012/9/contents) και ο νόμος του 2016 για τις ερευνητικές εξουσίες (Investigatory Powers Act, IPA), ο οποίος διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2016/25/contents), ii) για τη Σκωτία, ο νόμος του 2016 για την ποινική δικαιοσύνη (Σκωτία) (Criminal Justice (Scotland) Act 2016), ο οποίος διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/asp/2016/1/contents και ο νόμος του 1995 για την ποινική δικονομία (Σκωτία), ο οποίος διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/1995/46/contents), iii) για τη Βόρεια Ιρλανδία, το διάταγμα του 1989 για την αστυνομία και τα αποδεικτικά στοιχεία σε ποινικές διαδικασίες (Βόρεια Ιρλανδία) (Police and Criminal Evidence (Northern Ireland) Order 1989), το οποίο διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/nisi/1989/1341/contents.

([50]) Οι αρχές του Ηνωμένου Βασιλείου εξήγησαν ότι η υπεροχή του γραπτού δικαίου είναι από μακρού εδραιωμένη στο Ηνωμένο Βασίλειο, ήδη από την απόφαση που ελήφθη στην υπόθεση Entick κατά Carrington [1765] EWHC KB J98, με την οποία αναγνωρίστηκε ότι υπήρχαν όρια στην άσκηση των εξουσιών από την εκτελεστική εξουσία και θεσπίστηκε η αρχή ότι οι εξουσίες που απορρέουν από το κοινοδίκαιο, καθώς και οι εξουσίες που πηγάζουν από τα προνόμια του μονάρχη και της κυβέρνησης υπάγονται στους νόμους του κράτους.

([51]) Βλέπε υπόθεση Rice κατά Connolly [1966] 2 QB 414.

([52]) Βλέπε υπόθεση R(Catt) κατά Association of Chief police Officers [2015] AC 1065, όπου σε σχέση με την εξουσία της αστυνομίας να λαμβάνει και να διατηρεί τις πληροφορίες ενός ατόμου (που είχε διαπράξει έγκλημα), ο δικαστής Λόρδος Sumption έκρινε ότι βάσει του κοινοδικαίου, η αστυνομία έχει την εξουσία να λαμβάνει και να αποθηκεύει πληροφορίες για σκοπούς αστυνόμευσης, δηλαδή, εν γένει, για τη διατήρηση της δημόσιας τάξης και την πρόληψη και ανίχνευση εγκλημάτων. Αυτές οι εξουσίες δεν επιτρέπουν τη χρήση επεμβατικών μεθόδων λήψης πληροφοριών, όπως είσοδο σε ιδιωτική περιουσία ή ενέργειες (εκτός της σύλληψης βάσει εξουσιών που απορρέουν από το κοινοδίκαιο) που θα συνιστούσαν επίθεση. Ο δικαστής έκρινε ότι σ' αυτή την περίπτωση, οι εξουσίες που απορρέουν από το κοινοδίκαιο αρκούσαν σε μεγάλο βαθμό για να επιτραπεί η λήψη και η αποθήκευση των εν λόγω δημόσιων πληροφοριών σχετικά με τις συγκεκριμένες προσφυγές.

([53]) Νόμος του 2010 για την ισότητα, διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2010/15/contents.

([54]) Για παράδειγμα περίπτωσης στην οποία οι εξουσίες της αστυνομίας βάσει του κοινοδικαίου αξιολογούνται στο πλαίσιο του DPA 1998, βλέπε την απόφαση του ανώτερου δικαστηρίου στην υπόθεση Bridges κατά Chief Constable of South Wales Police (βλέπε υποσημείωση 33). Βλέπε επίσης υποθέσεις Vidal-Hall κατά Google Inc [2015] EWCA Civ 311 και Richard κατά BBC [2018] EWHC 1837 (Ch).

([55]) Βλέπε για παράδειγμα την καθοδήγηση της Αστυνομικής Υπηρεσίας της Βόρειας Ιρλανδίας (Police Service of Northern Ireland, PSNI) σχετικά με την υπηρεσιακή οδηγία για τη διαχείριση αρχείων (Records management service instruction), η οποία διατίθεται στον ακόλουθο σύνδεσμο: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service-procedures/records-management-080819.pdf.

([56]) Η Βουλή των Κοινοτήτων δημοσίευσε ενημερωτικό έγγραφο στο οποίο καθορίζονται οι βασικές εξουσίες της αστυνομίας στην Αγγλία και την Ουαλία βάσει του κοινοδικαίου και των νόμων (βλέπε https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). Σύμφωνα με το έγγραφο αυτό, για παράδειγμα, παρότι οι εξουσίες διατήρησης «της ειρήνης του Στέμματος» είναι εξουσίες που απορρέουν από το κοινοδίκαιο, όπως και η «χρήση βίας», «οι εξουσίες εξακρίβωσης στοιχείων και σωματικής έρευνας» απορρέουν πάντοτε από τον νόμο. Επιπλέον, η κυβέρνηση της Σκωτίας παρέχει πληροφορίες στον ιστότοπό της σχετικά με τις εξουσίες σύλληψης, εξακρίβωσης στοιχείων και σωματικής έρευνας που διαθέτει η αστυνομία (βλέπε https://www.gov.scot/policies/police/police-powers/).

([57]) Σύμφωνα με τις πληροφορίες που παρασχέθηκαν από τις αρχές του Ηνωμένου Βασιλείου, οι εξουσίες που απορρέουν από τα βασιλικά προνόμια και ασκούνται από την κυβέρνηση περιλαμβάνουν, για παράδειγμα, τη σύναψη και κύρωση συνθηκών, τη διεξαγωγή διπλωματίας και τη χρήση των ενόπλων δυνάμεων εντός του Ηνωμένου Βασιλείου για τη διατήρηση της ειρήνης προς υποστήριξη της αστυνομίας.

σκοπούς επιβολής του νόμου και η εξουσία κοινοποίησης δεδομένων μ' αυτόν τον τρόπο δεν ορίζεται πάντα με νόμο ([58]). Τα βασιλικά προνόμια δεσμεύονται από τις αρχές του κοινοδικαίου ([59]) και υπάγονται στον νόμο, ως εκ τούτου υπόκεινται στα όρια που προβλέπονται από τον νόμο του 1998 για τα ανθρώπινα δικαιώματα και από τον DPA 2018 ([60]).

(33) Όπως και στο άρθρο 8 της οδηγίας (ΕΕ) 2016/680, το καθεστώς του Ηνωμένου Βασιλείου απαιτεί από τις αρμόδιες αρχές, προκειμένου να συμμορφώνονται με την αρχή της νομιμότητας, να διασφαλίζουν ότι όταν η επεξεργασία βασίζεται στον νόμο, πρέπει να είναι επίσης «απαραίτητο» να εκτελούν το καθήκον που ασκείται για σκοπούς επιβολής του νόμου. Το ICO παρέχει καθοδήγηση σχετικά με το θέμα αυτό διευκρινίζοντας ότι «πρέπει να είναι ένας στοχευμένος και αναλογικός τρόπος για την επίτευξη του σκοπού. Η νόμιμη βάση δεν ισχύει εάν μπορείτε να επιτύχετε εύλογα τον σκοπό με άλλα λιγότερο παρεμβατικά μέσα. Δεν αρκεί το επιχείρημα ότι η επεξεργασία είναι αναγκαία επειδή έχετε επιλέξει να ασκήσετε τα καθήκοντά σας με συγκεκριμένο τρόπο. Το ερώτημα είναι αν η επεξεργασία είναι αναγκαία για τον δηλωθέντα σκοπό» ([61]).

2.4.1.2. Επεξεργασία βάσει της «συγκατάθεσης» του υποκειμένου των δεδομένων

(34) Όπως αναφέρεται στην αιτιολογική σκέψη (28), το άρθρο 35 παράγραφος 2 του DPA 2018 προβλέπει τη δυνατότητα επεξεργασίας δεδομένων προσωπικού χαρακτήρα βάσει της «συγκατάθεσης» του προσώπου.

(35) Ωστόσο, η συγκατάθεση δεν φαίνεται να αποτελεί συναφή νομική βάση για τις πράξεις επεξεργασίας που εμπίπτουν στο πεδίο της παρούσας απόφασης. Μάλιστα, οι πράξεις επεξεργασίας που καλύπτονται από την παρούσα απόφαση θα αφορούν πάντα δεδομένα που έχουν διαβιβαστεί βάσει της οδηγίας (ΕΕ) 2016/680 από αρμόδια αρχή κράτους μέλους σε αρμόδια αρχή του Ηνωμένου Βασιλείου. Ως εκ τούτου, κατά κανόνα δεν περιλαμβάνουν το είδος άμεσης αλληλεπίδρασης (συλλογή) μεταξύ δημόσιας αρχής και των υποκειμένων των δεδομένων που μπορεί να βασίζεται στη συγκατάθεση σύμφωνα με το άρθρο 35 παράγραφος 2 στοιχείο a) του DPA 2018.

(36) Παρότι η βάση της συγκατάθεσης δεν θεωρείται, συνεπώς, συναφής για την αξιολόγηση που διενεργείται στο πλαίσιο της παρούσας απόφασης, αξίζει να σημειωθεί, χάριν πληρότητας, ότι στο πλαίσιο της επιβολής του νόμου η επεξεργασία δεν βασίζεται ποτέ αποκλειστικά στη συγκατάθεση, καθώς η αρμόδια αρχή πρέπει πάντοτε να βασίζεται σε υποκείμενη εξουσία η οποία της επιτρέπει να επεξεργάζεται τα δεδομένα ([62]). Πιο συγκεκριμένα, όπως προβλέπεται επίσης στην οδηγία (ΕΕ) 2016/680 ([63]), αυτό σημαίνει ότι η συγκατάθεση χρησιμεύει ως πρόσθετη προϋπόθεση για να καταστούν δυνατές ορισμένες περιορισμένες και συγκεκριμένες πράξεις επεξεργασίας οι οποίες σε διαφορετική περίπτωση δεν θα μπορούσαν να πραγματοποιηθούν, για παράδειγμα η συλλογή και επεξεργασία δείγματος DNA προσώπου που δεν είναι ύποπτο. Στην περίπτωση αυτή, η επεξεργασία δεν πραγματοποιείται εάν δεν παρασχεθεί συγκατάθεση ή εάν αυτή ανακληθεί ([64]).

([58]) Στο πλαίσιο αυτό, βλέπε την αξιολόγηση του καθεστώτος περαιτέρω διαβίβασης στο Ηνωμένο Βασίλειο στις αιτιολογικές σκέψεις (74)-(87).

([59]) Βλέπε υπόθεση Bancoult κατά Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, στην οποία τα δικαστήρια έκριναν ότι η εξουσία βάσει βασιλικών προνομίων για την έκδοση διαταγών στο Συμβούλιο υπόκειται επίσης στους συνήθεις λόγους άσκησης δικαστικού ελέγχου.

([60]) Βλέπε υπόθεση Attorney-General κατά De Keyser's Royal Hotel Ltd [1920] [1920] AC 508, όπου το δικαστήριο έκρινε ότι δεν μπορούν να ασκούνται εξουσίες βάσει βασιλικών προνομίων όταν αυτές αντικαθίστανται από εξουσίες που απορρέουν από τον νόμο· υπόθεση Laker Airways Ltd κατά Department of Trade [1977] QB 643, όπου το δικαστήριο έκρινε ότι δεν μπορούν να ασκούνται εξουσίες βάσει βασιλικών προνομίων προκειμένου να ματαιωθεί το γραπτό δίκαιο· υπόθεση R κατά Secretary of State for the Home Department, ex p. Fire Brigades Union [1995] UKHL 3, στην οποία το δικαστήριο έκρινε ότι δεν μπορούν να ασκούνται εξουσίες βάσει βασιλικών προνομίων όταν αυτές έρχονται σε αντίθεση με νομοθεσία που έχει θεσπιστεί, ακόμη και όταν η εν λόγω νομοθεσία δεν έχει αρχίσει ακόμη να ισχύει· υπόθεση R (Miller) κατά Secretary of State for Exiting the European Union [2017] UKSC 5, όπου το δικαστήριο επιβεβαίωσε την ικανότητα του γραπτού δικαίου να προσαρμόζει και να καταργεί εξουσίες που απορρέουν από τα βασιλικά προνόμια. Για γενική επισκόπηση της σχέσης μεταξύ των βασιλικών προνομίων και των εξουσιών που απορρέουν από τον νόμο ή το κοινοδίκαιο, βλέπε το ενημερωτικό έγγραφο της Βουλής των Κοινοτήτων, το οποίο διατίθεται στον ακόλουθο σύνδεσμο: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf.

([61]) Guide to Law Enforcement Processing, "What is the first principle about?", διαθέσιμος στον ακόλουθο σύνδεσμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2.

([62]) Αυτό προκύπτει από τη διατύπωση της σχετικής διάταξης του DPA 2018, σύμφωνα με την οποία η επεξεργασία δεδομένων προσωπικού χαρακτήρα για οποιονδήποτε από τους σκοπούς επιβολής του νόμου είναι σύννομη μόνον εφόσον «βασίζεται στο δίκαιο» και είτε — α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία για τον σκοπό αυτό, είτε β) η επεξεργασία είναι απαραίτητη για την εκτέλεση καθήκοντος που ασκείται για τον σκοπό αυτό από αρμόδια αρχή.

([63]) Βλέπε αιτιολογικές σκέψεις 35 και 37 της οδηγίας (ΕΕ) 2016/680.

([64]) Οι αρχές του Ηνωμένου Βασιλείου έχουν εξηγήσει ότι ένα παράδειγμα στο οποίο η συγκατάθεση μπορεί να αποτελεί κατάλληλη βάση για την επεξεργασία θα ήταν η περίπτωση κατά την οποία η αστυνομία λαμβάνει δείγμα DNA σε σχέση με αγνοούμενο πρόσωπο προκειμένου να το αντιστοιχίσει με σορό που έχει βρεθεί. Υπό αυτές τις συνθήκες, δεν θα ήταν σκόπιμο η αστυνομία να υποχρεώσει το υποκείμενο των δεδομένων να παράσχει δείγμα· αντίθετα, η αστυνομία θα πρέπει να ζητήσει τη συγκατάθεση του προσώπου, η οποία παρέχεται ελεύθερα και μπορεί να ανακληθεί ανά πάσα στιγμή. Εάν ανακληθεί η συγκατάθεση, τα δεδομένα δεν μπορούν πλέον να υποβληθούν σε επεξεργασία, εκτός εάν στοιχειοθετηθεί νέα νομική βάση για τη συνέχιση της επεξεργασίας του δείγματος (π.χ. το υποκείμενο των δεδομένων κατέστη ύποπτο). Περαιτέρω παράδειγμα θα μπορούσε να προκύψει σε περίπτωση που μια αστυνομική δύναμη ερευνά έγκλημα στο οποίο το θύμα (θα μπορούσε να είναι θύμα ληστείας, εγκλήματος κατά της γενετήσιας ελευθερίας, ενδοοικογενειακής βίας, συγγενής θύματος ανθρωποκτονίας ή άλλου θύματος εγκλήματος) θα μπορούσε να επωφεληθεί από παραπομπή στην οργάνωση στήριξης θυμάτων Victim Support (ανεξάρτητη κοινωφελής οργάνωση που έχει ως στόχο την υποστήριξη ανθρώπων που έχουν πληγεί από εγκληματικές πράξεις και τραυματικά περιστατικά). σ' αυτές τις περιστάσεις, η αστυνομία κοινοποιεί τις προσωπικές πληροφορίες, όπως το όνομα και τα στοιχεία επικοινωνίας, στην οργάνωση Victim Support μόνον εάν έχει τη συγκατάθεση του θύματος.

(37) Σε περιπτώσεις όπου απαιτείται η συγκατάθεση του προσώπου, η εν λόγω συγκατάθεση πρέπει να είναι αδιαμφισβήτητη και να περιλαμβάνει σαφή θετική ενέργεια ([65]). Οι αστυνομικές δυνάμεις υποχρεούνται να διαθέτουν δήλωση περί προστασίας της ιδιωτικότητας, η οποία περιλαμβάνει, μεταξύ άλλων, τις απαραίτητες πληροφορίες σχετικά με την έγκυρη χρήση της συγκατάθεσης. Επιπλέον, κάποιες από αυτές δημοσιεύουν πρόσθετο υλικό σχετικά με τον τρόπο με τον οποίο συμμορφώνονται με τη νομοθεσία για την προστασία των δεδομένων, συμπεριλαμβανομένου του τρόπου και του χρόνου χρήσης της συγκατάθεσης ως νομικής βάσης ([66]).

2.4.1.3. Επεξεργασία ευαίσθητων δεδομένων

(38) Θα πρέπει να προβλέπονται ειδικές εγγυήσεις για την επεξεργασία «ειδικών κατηγοριών δεδομένων». Στο πλαίσιο αυτό, όπως προβλέπεται και στο άρθρο 10 της οδηγίας (ΕΕ) 2016/680, το μέρος 3 του DPA 2018 προβλέπει ισχυρότερες εγγυήσεις για τη λεγόμενη «επεξεργασία ευαίσθητων δεδομένων» ([67]).

(39) Σύμφωνα με το άρθρο 35 παράγραφος 3 του DPA 1998, τα ευαίσθητα δεδομένα μπορούν να υποβάλλονται σε επεξεργασία από αρμόδιες αρχές για σκοπούς επιβολής του νόμου μόνο σε δύο περιπτώσεις: 1) το υποκείμενο των δεδομένων έχει παράσχει τη συγκατάθεσή του για την επεξεργασία για σκοπούς επιβολής του νόμου και τη στιγμή κατά την οποία πραγματοποιείται η επεξεργασία, ο υπεύθυνος επεξεργασίας διαθέτει έγγραφο κατάλληλης πολιτικής (appropriate policy document, APD) ([68])· ή 2) η επεξεργασία είναι απολύτως απαραίτητη για τον σκοπό της επιβολής του νόμου, η επεξεργασία πληροί τουλάχιστον μία από τις προϋποθέσεις του παραρτήματος 8 του DPA 2018, και τη στιγμή κατά την οποία πραγματοποιείται η επεξεργασία, ο υπεύθυνος επεξεργασίας διαθέτει έγγραφο κατάλληλης πολιτικής ([69]).

(40) Όσον αφορά την πρώτη περίπτωση και όπως εξηγείται στην αιτιολογική σκέψη 38, η βάση της συγκατάθεσης δεν θεωρείται συναφής στο είδος της κατάστασης διαβίβασης που υπόκειται στην παρούσα απόφαση ([70]).

(41) Όταν η επεξεργασία ευαίσθητων δεδομένων δεν βασίζεται στη συγκατάθεση, μπορεί να διεξάγεται με τη χρήση μίας από τις προϋποθέσεις που απαριθμούνται στο παράρτημα 8 του DPA 2018. Οι προϋποθέσεις αυτές αφορούν την επεξεργασία που είναι απαραίτητη για νόμιμους σκοπούς· για την απονομή δικαιοσύνης· για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου προσώπου· για την προστασία παιδιών και προσώπων που διατρέχουν κίνδυνο· για νομικές αξιώσεις· για δικαστικές πράξεις· για την πρόληψη της απάτης· για σκοπούς αρχειοθέτησης· όταν τα δεδομένα προσωπικού χαρακτήρα έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων. Εκτός από την περίπτωση

([65]) Δεν υπάρχει χωριστός ορισμός της «συγκατάθεσης» για τους σκοπούς της επεξεργασίας δεδομένων προσωπικού χαρακτήρα στο πλαίσιο του μέρους 3 του DPA 2018. Το ICO παρείχε καθοδήγηση σχετικά με την έννοια της «συγκατάθεσης» βάσει του μέρους 3 του DPA 2018, στην οποία διευκρινίζει ότι έχει την ίδια έννοια και θα πρέπει να εναρμονίζεται με τον ορισμό που παρέχει ο ΓΚΠΔ, και ειδικότερα ότι «η συγκατάθεση πρέπει να είναι ελεύθερη, συγκεκριμένη και εν πλήρει επιγνώσει και ότι πρέπει να υπάρχει πραγματική επιλογή σχετικά με τη συμφωνία για την επεξεργασία των δεδομένων» [Guide to Law Enforcement Processing, "What is the first principle about?" (βλέπε υποσημείωση 64) και Guide to Data Protection, ενότητα σχετικά με τη συγκατάθεση, διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Βλέπε, για παράδειγμα, τις πληροφορίες στην ιστοσελίδα της αστυνομίας του Lincolnshire (βλέπε https://www.lincs.police.uk/resource-library/data-protection/law-enforcement-processing/) ή στην ιστοσελίδα της αστυνομίας του West Yorkshire (βλέπε https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) Άρθρο 35 παράγραφος 8 του DPA 2018.

([68]) Άρθρο 35 παράγραφος 4 του DPA 2018.

([69]) Άρθρο 35 παράγραφος 5 του DPA 2018.

([70]) Για λόγους πληρότητας, αξίζει να σημειωθεί ότι όταν η επεξεργασία βασίζεται σε συγκατάθεση, αυτή θα πρέπει να είναι ελεύθερη, συγκεκριμένη και εν πλήρει επιγνώσει, και θα πρέπει να υπάρχει συγκεκριμένη επιλογή σχετικά με τη συμφωνία για την επεξεργασία των δεδομένων. Επιπλέον, ο υπεύθυνος επεξεργασίας, όταν προβαίνει στην επεξεργασία βάσει της «συγκατάθεσης» του υποκειμένου των δεδομένων, είναι υποχρεωμένος να διαθέτει «έγγραφο κατάλληλης πολιτικής» (APD). Στο άρθρο 42 του DPA 2018 περιγράφονται οι απαιτήσεις τις οποίες πρέπει να πληροί το APD. Ορίζεται σαφώς ότι το έγγραφο πρέπει, κατ' ελάχιστον, να επεξηγεί τις διαδικασίες που ακολουθεί ο υπεύθυνος επεξεργασίας για τη διασφάλιση της συμμόρφωσης με τις αρχές προστασίας των δεδομένων, καθώς και τις πολιτικές του υπευθύνου επεξεργασίας όσον αφορά τη διατήρηση και τη διαγραφή δεδομένων προσωπικού χαρακτήρα. Σύμφωνα με το άρθρο 42 του DPA 2018, αυτό σημαίνει ότι ο υπεύθυνος επεξεργασίας πρέπει να προσκομίσει έγγραφο το οποίο α) επεξηγεί τις διαδικασίες που ακολουθεί ο υπεύθυνος επεξεργασίας για τη διασφάλιση της συμμόρφωσης με τις αρχές προστασίας των δεδομένων· και β) επεξηγεί τις πολιτικές του υπευθύνου επεξεργασίας όσον αφορά τη διατήρηση και τη διαγραφή δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία βάσει συγκατάθεσης του υποκειμένου των δεδομένων ή παρέχει ένδειξη σχετικά με την πιθανή διάρκεια της διατήρησης των εν λόγω δεδομένων προσωπικού χαρακτήρα. Ειδικότερα, το έγγραφο πολιτικής απαιτεί από τον υπεύθυνο επεξεργασίας, κατά την τήρηση του καθήκοντος καταγραφής των δραστηριοτήτων επεξεργασίας, να συμπεριλαμβάνει πάντοτε τα στοιχεία που αναφέρονται στα στοιχεία α) και β). Το ICO έχει δημοσιεύσει υπόδειγμα εγγράφου (Guide to Law Enforcement Processing. "Conditions for sensitive processing", διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/conditions-for-sensitive-processing) και μπορεί να λαμβάνει μέτρα επιβολής εάν οι υπεύθυνοι επεξεργασίας δεν τηρούν αυτές τις απαιτήσεις. Το APD εξετάζεται επίσης από τα δικαστήρια κατά την εξέταση πιθανών παραβάσεων του DPA 2018. Για παράδειγμα, στην πρόσφατη υπόθεση R (Bridges) κατά Chief Constable of South Wales Police, τα δικαστήρια εξέτασαν το APD του υπευθύνου επεξεργασίας και έκριναν ότι ήταν επαρκές αλλά θα ήταν χρήσιμο αν περιείχε περισσότερες λεπτομέρειες. Ως εκ τούτου, η αστυνομία της Νότιας Ουαλίας επανεξέτασε το APD και το επικαιροποίησε σύμφωνα με τις νέες οδηγίες του ICO (βλέπε υποσημείωση 33). Επιπλέον, σύμφωνα με το άρθρο 42 παράγραφος 3 του DPA 2018, το APD θα πρέπει να τελεί υπό τακτική επανεξέταση από τον υπεύθυνο επεξεργασίας. Τέλος, ως πρόσθετη διασφάλιση, σύμφωνα με το άρθρο 42 παράγραφος 4 του DPA 2018, ο υπεύθυνος επεξεργασίας είναι υποχρεωμένος να τηρεί επαυξημένο αρχείο των δραστηριοτήτων επεξεργασίας, συμπεριλαμβανομένων πρόσθετων στοιχείων σε σύγκριση με τη γενική υποχρέωση του υπευθύνου επεξεργασίας να τηρεί αρχεία των δραστηριοτήτων επεξεργασίας, όπως καθορίζεται στο άρθρο 61 του DPA 2018.

κατά την οποία τα δεδομένα έχουν προδήλως δημοσιοποιηθεί, όλες οι προϋποθέσεις που προβλέπονται στο παράρτημα 8 υπόκεινται σε έλεγχο «αυστηρώς αναγκαίου χαρακτήρα». Όπως διευκρινίζει το ICO, «ο αυστηρώς αναγκαίος χαρακτήρας σ' αυτό το πλαίσιο σημαίνει ότι η επεξεργασία πρέπει να σχετίζεται με επιτακτική κοινωνική ανάγκη, και δεν είναι ευλόγως δυνατή η επίτευξή της με λιγότερο παρεμβατικά μέσα» ([71]). Επιπλέον, κάποιες από τις προϋποθέσεις υπόκεινται σε πρόσθετους περιορισμούς. Για παράδειγμα, για να γίνει επίκληση της προϋπόθεσης των «νόμιμων σκοπών» και της «προϋπόθεσης προστασίας» (παράρτημα 8 παράγραφος 1 και παράγραφος 4), πρέπει να πληρούται ένα πρόσθετο κριτήριο ουσιαστικού δημόσιου συμφέροντος. Επιπλέον, σε σχέση με τις προϋποθέσεις που αφορούν την προστασία του παιδιού (παράρτημα 8 παράγραφος 4), το υποκείμενο των δεδομένων πρέπει επίσης να είναι συγκεκριμένης ηλικίας και να θεωρείται ότι διατρέχει κίνδυνο. Επιπλέον, ο υπεύθυνος επεξεργασίας μπορεί να εφαρμόσει την προϋπόθεση που προβλέπεται στο παράρτημα 8 παράγραφος 4 μόνο σε ειδικές περιστάσεις ([72]). Ομοίως, υπάρχουν περιορισμοί για τις προϋποθέσεις των «δικαστικών πράξεων» και της «πρόληψης της απάτης» (παράρτημα 8 παράγραφοι 7 και 8, αντίστοιχα). Και οι δύο ισχύουν μόνο για συγκεκριμένους υπευθύνους επεξεργασίας. Στην περίπτωση των δικαστικών πράξεων, μόνο δικαστήριο ή άλλη δικαστική αρχή μπορεί να χρησιμοποιήσει την προϋπόθεση αυτή, ενώ στην περίπτωση της πρόληψης της απάτης μόνον οι υπεύθυνοι επεξεργασίας που είναι οργανώσεις καταπολέμησης της απάτης μπορούν να βασίζονται στην προϋπόθεση αυτή.

(42) Τέλος, όταν η επεξεργασία βασίζεται σε μία από τις προϋποθέσεις που απαριθμούνται στο παράρτημα 8 και, αντίστοιχα, σύμφωνα με το άρθρο 42 του DPA 2018, θα πρέπει να υπάρχει «έγγραφο κατάλληλης πολιτικής» —το οποίο επεξηγεί τις διαδικασίες που ακολουθεί ο υπεύθυνος επεξεργασίας για τη διασφάλιση της συμμόρφωσης με τις αρχές προστασίας των δεδομένων και τις πολιτικές που ακολουθεί όσον αφορά τη διατήρηση και τη διαγραφή δεδομένων— ενώ εφαρμόζονται επίσης υποχρεώσεις τήρησης επαυξημένου αρχείου.

2.4.2. *Περιορισμός του σκοπού*

(43) Τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία για συγκεκριμένο σκοπό και στη συνέχεια να χρησιμοποιούνται μόνο στο μέτρο που αυτό δεν είναι ασύμβατο με τον σκοπό της επεξεργασίας. Αυτή η αρχή προστασίας των δεδομένων κατοχυρώνεται στο άρθρο 36 του DPA 2018. Η διάταξη αυτή, όπως και το άρθρο 4 παράγραφος 1 στοιχείο β) της οδηγίας (ΕΕ) 2016/680, προβλέπει ότι α) ο σκοπός επιβολής του νόμου για τον οποίο συλλέγονται σε κάθε περίσταση τα δεδομένα προσωπικού χαρακτήρα θα πρέπει να είναι καθορισμένος, ρητός και νόμιμος, και β) τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται με τον τρόπο αυτό δεν πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο ασύμβατο προς τον σκοπό για τον οποίο συλλέχθηκαν.

(44) Όταν οι αρμόδιες αρχές επεξεργάζονται δεδομένα για σκοπούς επιβολής του νόμου, η επεξεργασία αυτή μπορεί να περιλαμβάνει σκοπούς αρχειοθέτησης, επιστημονικής ή ιστορικής έρευνας και στατιστικούς σκοπούς ([73]). Σ' αυτές τις περιπτώσεις, ο DPA 2018 διευκρινίζει επίσης ότι η αρχειοθέτηση (ή η επεξεργασία για επιστημονική ή ιστορική έρευνα και στατιστικούς σκοπούς) δεν επιτρέπεται όταν πραγματοποιείται σε σχέση με αποφάσεις που λαμβάνονται για συγκεκριμένο υποκείμενο δεδομένων ή εάν αυτή ενδέχεται να του προκαλέσει σημαντική ζημία ή οδύνη ([74]).

2.4.3. *Ακρίβεια και ελαχιστοποίηση των δεδομένων*

(45) Τα δεδομένα πρέπει να είναι ακριβή και, όταν χρειάζεται, να επικαιροποιούνται. Πρέπει επίσης να είναι κατάλληλα, συναφή και όχι υπερβολικά σε σχέση με τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία. Όπως και στο άρθρο 4 παράγραφος 1 στοιχεία γ), δ) και ε) της οδηγίας (ΕΕ) 2016/680, οι αρχές αυτές διασφαλίζονται στα άρθρα 37 και 38 του DPA 2018. Θα πρέπει να λαμβάνονται όλα τα εύλογα μέτρα ώστε να διασφαλίζεται ότι δεδομένα προσωπικού χαρακτήρα που είναι ανακριβή ([75]) διαγράφονται ή

([71]) Guide to Law Enforcement Processing, "Conditions for sensitive processing" (βλέπε υποσημείωση 70).

([72]) Η επεξεργασία διενεργείται χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων όταν: α) δεν μπορεί να δοθεί συγκατάθεση για την επεξεργασία από το υποκείμενο των δεδομένων· β) δεν μπορεί ευλόγως να αναμένεται από τον υπεύθυνο επεξεργασίας να λάβει τη συγκατάθεση του υποκειμένου των δεδομένων για την επεξεργασία· γ) η επεξεργασία πρέπει να πραγματοποιηθεί χωρίς τη συγκατάθεση του υποκειμένου των δεδομένων επειδή η λήψη της συγκατάθεσης του υποκειμένου των δεδομένων θα έθιγε την παροχή της προστασίας που αναφέρεται στο εδάφιο 1 στοιχείο α).

([73]) Βλέπε άρθρο 41 παράγραφος 1 του DPA 2018.

([74]) Βλέπε άρθρο 41 παράγραφος 2 του DPA 2018.

([75]) Το άρθρο 205 του DPA 2018 ορίζει τον όρο «ανακριβή» ως «εσφαλμένα ή παραπλανητικά» δεδομένα προσωπικού χαρακτήρα. Οι αρχές του Ηνωμένου Βασιλείου έχουν εξηγήσει ότι είναι σύνηθες τα δεδομένα που σχετίζονται με ποινικές έρευνες να είναι συχνά ελλιπή αλλά ότι μπορούν να είναι ακριβή ανεξαρτήτως αυτού.

διορθώνονται χωρίς καθυστέρηση ([76]), λαμβανομένου υπόψη του σκοπού επιβολής του νόμου για τον οποίο υποβάλλονται σε επεξεργασία ([77]), καθώς και να διασφαλίζεται ότι δεδομένα προσωπικού χαρακτήρα που είναι ανακριβή, ελλιπή ή δεν είναι πλέον επικαιροποιημένα δεν διαβιβάζονται ούτε καθίστανται διαθέσιμα για κανέναν από τους σκοπούς επιβολής του νόμου ([78]).

(46) Επιπλέον, όπως και στο άρθρο 7 της οδηγίας (ΕΕ) 2016/680, το καθεστώς προστασίας δεδομένων του Ηνωμένου Βασιλείου προβλέπει ότι τα δεδομένα προσωπικού χαρακτήρα που βασίζονται σε πραγματικά περιστατικά πρέπει, στο μέτρο του δυνατού, να διακρίνονται από τα δεδομένα προσωπικού χαρακτήρα που βασίζονται σε προσωπικές εκτιμήσεις ([79]). Κατά περίπτωση και στο μέτρο του δυνατού, πρέπει να γίνεται σαφής διάκριση μεταξύ των δεδομένων προσωπικού χαρακτήρα που αφορούν διαφορετικές κατηγορίες υποκειμένων των δεδομένων, όπως υπόπτους, πρόσωπα που έχουν καταδικαστεί για ποινικό αδίκημα, θύματα ποινικών αδικημάτων και μάρτυρες ([80]).

2.4.4. *Περιορισμός του χρόνου αποθήκευσης*

(47) Σύμφωνα με το άρθρο 5 της οδηγίας (ΕΕ) 2016/680, τα δεδομένα θα πρέπει, καταρχήν, να διατηρούνται μόνο για χρονικό διάστημα που δεν υπερβαίνει τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα. Σύμφωνα με το άρθρο 39 του DPA 2018, και όπως προβλέπεται και στο άρθρο 5 της εν λόγω οδηγίας, απαγορεύεται η διατήρηση δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία για οποιονδήποτε από τους σκοπούς επιβολής του νόμου για διάστημα που υπερβαίνει το αναγκαίο σε σχέση με τον σκοπό για τον οποίο υποβάλλονται σε επεξεργασία. Το νομικό καθεστώς του Ηνωμένου Βασιλείου απαιτεί τη θέσπιση κατάλληλων προθεσμιών για την περιοδική επανεξέταση της αναγκαιότητας συνεχούς αποθήκευσης δεδομένων προσωπικού χαρακτήρα για οποιονδήποτε από τους σκοπούς επιβολής του νόμου. Στη σχετική νομοθεσία και στις οδηγίες που διέπουν τις εξουσίες και τη λειτουργία της αστυνομίας έχουν θεσπιστεί περαιτέρω κανόνες σχετικά με τις πρακτικές που αφορούν τη διατήρηση δεδομένων προσωπικού χαρακτήρα και τις εφαρμοστέες προθεσμίες. Για παράδειγμα, στην Αγγλία και την Ουαλία, ο κώδικας ορθής πρακτικής MoPI του Σώματος των Εργαζομένων στην Αστυνόμευση, μαζί με το έγγραφο καθοδήγησης APP για τη διαχείριση πληροφοριών της αστυνομίας, παρέχουν ένα πλαίσιο για τη διασφάλιση μιας συνεπούς διαδικασίας διατήρησης, επανεξέτασης και διάθεσης βάσει κινδύνου για τη διαχείριση των επιχειρησιακών πληροφοριών αστυνόμευσης ([81]). Το πλαίσιο αυτό δημιουργεί σαφείς προσδοκίες σε ολόκληρη την υπηρεσία όσον αφορά τον τρόπο με τον οποίο οι πληροφορίες θα πρέπει να δημιουργούνται, να ανταλλάσσονται, να χρησιμοποιούνται και να αποτελούν αντικείμενο διαχείρισης εντός και μεταξύ των επιμέρους αστυνομικών δυνάμεων και άλλων υπηρεσιών ([82]). Η αστυνομία θα πρέπει να συμμορφώνεται με τον κώδικα ορθής πρακτικής και η συμμόρφωσή της επαληθεύεται από την Επιθεώρηση Αστυνομικών, Πυροσβεστικών και Διασωστικών Υπηρεσιών του Ηνωμένου Βασιλείου ([83]).

(48) Η Αστυνομική Υπηρεσία της Βόρειας Ιρλανδίας (PSNI) δεν έχει εκ του νόμου υποχρέωση να τηρεί τον κώδικα ορθής πρακτικής MoPI. Ωστόσο, το πλαίσιο MoPI που εγκρίθηκε το 2011 συμπληρώνεται με εγχειρίδιο της PSNI ([84]), το οποίο καθορίζει τις πολιτικές και τις διαδικασίες σχετικά με τον τρόπο εφαρμογής του κώδικα ορθής πρακτικής MoPI στη Βόρεια Ιρλανδία.

([76]) Άρθρο 38 παράγραφος 1 στοιχείο b) του DPA 2018.

([77]) Σύμφωνα με το επεξηγηματικό πλαίσιο του Ηνωμένου Βασιλείου για τη συζήτηση σχετικά με την επάρκεια (UK Explanatory Framework for Adequacy Discussions), «αυτό διασφαλίζει την αναγνώριση τόσο των δικαιωμάτων των υποκειμένων των δεδομένων όσο και των επιχειρησιακών αναγκών των υπηρεσιών επιβολής του νόμου. Το ανωτέρω σημείο εξετάστηκε προσεκτικά κατά τα στάδια σύνταξης του νομοσχεδίου για την προστασία των δεδομένων, καθώς ενδέχεται να υπάρχουν συγκεκριμένοι και περιορισμένοι επιχειρησιακοί λόγοι για τους οποίους τα δεδομένα δεν μπορούν να διορθωθούν. Αυτό πιθανότατα συμβαίνει εάν τα ανακριβή δεδομένα προσωπικού χαρακτήρα πρέπει να διατηρηθούν στην αρχική τους μορφή για αποδεικτικούς σκοπούς» (βλέπε UK Explanatory Framework for Adequacy Discussions, section F: Law Enforcement, σ. 21, βλέπε υποσημείωση 9).

([78]) Άρθρο 38 παράγραφος 4 του DPA 2018. Επιπλέον, σύμφωνα με το άρθρο 38 παράγραφος 5 του DPA 2018, πρέπει να επαληθεύεται η ποιότητα των δεδομένων προσωπικού χαρακτήρα πριν αυτά διαβιβαστούν ή καταστούν διαθέσιμα, σε κάθε διαβίβαση δεδομένων προσωπικού χαρακτήρα, πρέπει να περιλαμβάνονται οι απαραίτητες πληροφορίες που επιτρέπουν στον αποδέκτη να αξιολογήσει τον βαθμό ακρίβειας, πληρότητας και αξιοπιστίας των δεδομένων και τον βαθμό επικαιροποίησής τους, και αν, μετά τη διαβίβαση των δεδομένων προσωπικού χαρακτήρα, προκύψει ότι τα δεδομένα ήταν εσφαλμένα ή ότι η διαβίβαση ήταν παράνομη, ο αποδέκτης πρέπει να ενημερώνεται χωρίς καθυστέρηση.

([79]) Άρθρο 38 παράγραφος 2 του DPA 2018.

([80]) Άρθρο 38 παράγραφος 3 του DPA 2018.

([81]) Το πλαίσιο αυτό διασφαλίζει τη συνέπεια στην εφαρμογή της αποθήκευσης των δεδομένων προσωπικού χαρακτήρα που αποκτώνται. Η περίοδος επανεξέτασης εξαρτάται από τα αδικήματα, τα οποία διακρίνονται σε 4 κατηγορίες: 1) ορισμένα ζητήματα δημόσιας προστασίας· 2) άλλα βίαια και σοβαρά αδικήματα κατά της γενετήσιας ελευθερίας· 3) όλα τα άλλα αδικήματα· 4) διάφορα. Περισσότερες λεπτομέρειες διατίθενται στο έγγραφο καθοδήγησης APP για τη διαχείριση πληροφοριών της αστυνομίας (βλέπε υποσημείωση 26).

([82]) Σύμφωνα με τις πληροφορίες που παρασχέθηκαν από τις αρχές του Ηνωμένου Βασιλείου, και άλλοι οργανισμοί είναι ελεύθεροι να τηρούν τις αρχές του κώδικα ορθής πρακτικής MoPI, εάν το επιθυμούν – για παράδειγμα, η Φορολογική και Τελωνειακή Αρχή του Ηνωμένου Βασιλείου και η Εθνική Υπηρεσία Δίωξης του Εγκλήματος υιοθετούν οικειοθελώς πολλές από τις αρχές του κώδικα ορθής πρακτικής MoPI προκειμένου να διασφαλίζεται συνέπεια μεταξύ των αρχών επιβολής του νόμου. Κατά γενικό κανόνα, οι περισσότεροι οργανισμοί παρέχουν στο προσωπικό τους ειδικές πολιτικές και καθοδήγηση για όλο το προσωπικό σχετικά με τον τρόπο χειρισμού των δεδομένων στο πλαίσιο του ρόλου τους, ειδικά σχεδιασμένες για τον συγκεκριμένο οργανισμό. Αυτές οι πολιτικές και η καθοδήγηση συνήθως περιλαμβάνουν και υποχρεωτική κατάρτιση.

([83]) Ο κώδικας ορθής πρακτικής MoPI εκδόθηκε βάσει των εξουσιών που προβλέπονται από τον νόμο του 1996 για την αστυνομία, ο οποίος παρέχει στο Σώμα των Εργαζομένων στην Αστυνόμευση τη δυνατότητα να εκδίδει κώδικες ορθής πρακτικής για την αποτελεσματική λειτουργία της αστυνόμευσης. Κάθε κώδικας ορθής πρακτικής που καταρτίζεται δυνάμει του συγκεκριμένου νόμου πρέπει να έχει την έγκριση του ανώτερου υπουργού και υπόκειται σε διαβούλευση με την Εθνική Υπηρεσία Δίωξης του Εγκλήματος πριν υποβληθεί στο Κοινοβούλιο. Βάσει του άρθρου 39A παράγραφος 7 του νόμου του 1996 για την αστυνομία, η αστυνομία είναι υποχρεωμένη να λαμβάνει δεόντως υπόψη τους κώδικες που εκδίδονται δυνάμει του συγκεκριμένου νόμου.

([84]) Εγχειρίδιο MoPI της PSNI, Κεφάλαια 1-6.

(49) Στη Σκωτία, οι αστυνομικές δυνάμεις βασίζονται στην τυποποιημένη διαδικασία λειτουργίας για τη διατήρηση αρχείων (Record Retention Standard Operating Procedure, SOP) ([85]) η οποία υποστηρίζει την πολιτική διαχείρισης αρχείων (Records Management Policy) ([86]) της Αστυνομικής Υπηρεσίας της Σκωτίας. Η SOP ορίζει ειδικούς κανόνες διατήρησης για τα αρχεία που τηρεί η αστυνομία της Σκωτίας.

(50) Εκτός από τη γενική απαίτηση επανεξέτασης των αρχείων, η οποία ισχύει σε ολόκληρο το Ηνωμένο Βασίλειο, στους τοπικούς κανόνες παρέχονται περισσότερες λεπτομέρειες. Για παράδειγμα, όσον αφορά την Αγγλία και την Ουαλία, ο νόμος για την αστυνομία και τα αποδεικτικά στοιχεία σε ποινικές διαδικασίες, όπως τροποποιήθηκε με τον νόμο του 2012 για την προστασία των ελευθεριών (PoFA), προβλέπει τη διατήρηση δακτυλικών αποτυπωμάτων και προφίλ DNA, καθώς και ειδικό καθεστώς για τα πρόσωπα που δεν έχουν καταδικαστεί ([87]). Με τον PoFA δημιουργήθηκε επίσης η θέση του Επιτρόπου για τη Διατήρηση και Χρήση Βιομετρικού Υλικού (στο εξής: Επίτροπος Βιομετρικών Στοιχείων) ([88]). Στην επισκόπηση εικόνων κράτησης του 2017 ορίζονται ειδικοί κανόνες σχετικά με τις εικόνες κράτησης ([89]). Όσον αφορά τη Σκωτία, ο νόμος του 1995 για την ποινική δικονομία (Σκωτία) προβλέπει τους κανόνες για τη λήψη και τη διατήρηση δακτυλικών αποτυπωμάτων και βιολογικών δειγμάτων ([90]). Όπως και στην περίπτωση της Αγγλίας και της Ουαλίας, η νομοθεσία ρυθμίζει τη διατήρηση των βιομετρικών δεδομένων σε διάφορες περιπτώσεις ([91]).

2.4.5. *Ασφάλεια δεδομένων*

(51) Τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ασφάλειά τους, συμπεριλαμβανομένης της προστασίας τους από μη εγκεκριμένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά. Για τον σκοπό αυτό, οι δημόσιες αρχές πρέπει να λαμβάνουν τα κατάλληλα τεχνικά ή οργανωτικά μέτρα για την προστασία των δεδομένων προσωπικού χαρακτήρα από πιθανές απειλές. Τα μέτρα αυτά πρέπει να αξιολογούνται με βάση την πιο προηγμένη τεχνολογία και το σχετικό κόστος.

(52) Οι αρχές αυτές αντικατοπτρίζονται στο άρθρο 40 του DPA 2018, σύμφωνα με το οποίο, όπως προβλέπεται και στο άρθρο 4 παράγραφος 1 στοιχείο στ) της οδηγίας (ΕΕ) 2016/680, τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία για οποιονδήποτε από τους σκοπούς επιβολής του νόμου πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να εγγυάται τη δέουσα ασφάλεια των δεδομένων προσωπικού χαρακτήρα, με χρήση κατάλληλων τεχνικών ή

([85]) Record Retention Standard Operating Procedure (SOP), διατίθεται στον ακόλουθο σύνδεσμο: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf.

([86]) Για περισσότερες λεπτομέρειες σχετικά με τη διαχείριση των αρχείων, βλέπε πληροφορίες σχετικά με την Εθνική Υπηρεσία Αρχείων της Σκωτίας (National Records of Scotland), που διατίθενται στον ακόλουθο σύνδεσμο: https://www.nrscotland.gov.uk/record-keeping/records-management.

([87]) Η περίοδος διατήρησης ποικίλλει ανάλογα με το αν το πρόσωπο έχει καταδικαστεί ή όχι (άρθρα 63I – 63KI του PACE 1984). Για παράδειγμα, στην περίπτωση ενηλίκου που έχει καταδικαστεί για αδίκημα που εγγράφεται στο μητρώο, τα δακτυλικά του αποτυπώματα και το προφίλ DNA του μπορούν να διατηρηθούν επ' αόριστον (άρθρο 63I παράγραφος 2 του PACE 1984), ενώ η διατήρηση είναι χρονικά περιορισμένη εάν το καταδικασθέν πρόσωπο είναι κάτω των 18 ετών, το αδίκημα είναι «ήσσονος βαρύτητας» που εγγράφεται στο μητρώο και το εν λόγω πρόσωπο δεν έχει καταδικαστεί προηγουμένως (άρθρο 63K του PACE 1984). Η διατήρηση στην περίπτωση προσώπου που έχει συλληφθεί ή εις βάρος του οποίου έχουν απαγγελθεί κατηγορίες αλλά δεν έχει καταδικαστεί, περιορίζεται χρονικά σε τρία έτη (άρθρο 63F του PACE 1984). Η παράταση αυτής της περιόδου διατήρησης πρέπει να εγκριθεί από δικαστική αρχή (άρθρο 63F παράγραφος 7 του PACE 1984). Στην περίπτωση προσώπων που συλλαμβάνονται ή εις βάρος των οποίων απαγγέλλονται κατηγορίες για αδίκημα ήσσονος βαρύτητας, δεν είναι δυνατή η διατήρηση (άρθρο 63D και άρθρο 63H του PACE 1984).

([88]) Με το άρθρο 20 του PoFA 2012 δημιουργείται η θέση του Επιτρόπου Βιομετρικών Στοιχείων. Μεταξύ άλλων καθηκόντων, ο Επίτροπος Βιομετρικών Στοιχείων αποφασίζει αν η αστυνομία μπορεί να διατηρεί αρχεία προφίλ DNA και δακτυλικά αποτυπώματα που λαμβάνονται από πρόσωπα που έχουν συλληφθεί αλλά δεν τους έχουν απαγγελθεί κατηγορίες για αδίκημα που πληροί τις προϋποθέσεις (άρθρο 63G του PACE 1984). Επιπλέον, ο Επίτροπος Βιομετρικών Στοιχείων έχει γενική ευθύνη να ελέγχει τη διατήρηση και τη χρήση DNA και δακτυλικών αποτυπωμάτων, καθώς και τη διατήρηση για λόγους εθνικής ασφάλειας (άρθρο 20 παράγραφος 2 του PoFA 2012). Ο Επίτροπος Βιομετρικών Στοιχείων διορίζεται βάσει του κώδικα για τους δημόσιους διορισμούς (ο κώδικας είναι διαθέσιμος στον ακόλουθο σύνδεσμο: Governance Code for Public Appointments - GOV.UK (www.gov.uk)) και οι όροι του διορισμού του καθιστούν σαφές ότι μπορεί να παυθεί από τα καθήκοντά του από τον υπουργό Εσωτερικών μόνο σε αυστηρά καθορισμένες περιπτώσεις· σ' αυτές περιλαμβάνονται η μη εκτέλεση των καθηκόντων του για διάστημα τριών μηνών, η καταδίκη του για ποινικό αδίκημα ή η μη συμμόρφωσή του με τους όρους του διορισμού του.

([89]) Review of the Use and Retention of Custody Images, διατίθεται στον ακόλουθο σύνδεσμο: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention.

([90]) Άρθρα 18 και επόμενα του νόμου του 1995 για την ποινική δικονομία (Σκωτία).

([91]) Οι περίοδοι διατήρησης ποικίλλουν ανάλογα με το αν το πρόσωπο έχει καταδικαστεί [άρθρο 18 παράγραφος 3 του νόμου του 1995 για την ποινική δικονομία (Σκωτία)] ή αν είναι ανήλικο. Στη δεύτερη περίπτωση, η περίοδος διατήρησης είναι 3 έτη από την έκδοση της καταδικαστικής απόφασης σε δίκες ανηλίκων [άρθρο 18E παράγραφος 8 του νόμου του 1995 για την ποινική δικονομία (Σκωτία)]. Δεν είναι δυνατή η διατήρηση δεδομένων προσώπων που έχουν συλληφθεί αλλά δεν τους έχουν απαγγελθεί κατηγορίες [άρθρο 18 παράγραφος 3 του νόμου του 1995 για την ποινική δικονομία (Σκωτία)], πλην ειδικών περιπτώσεων ανάλογα με τη σοβαρότητα του εγκλήματος [άρθρο 18A του νόμου του 1995 για την ποινική δικονομία (Σκωτία)]. Ο νόμος του 2020 για τον Επίτροπο Βιομετρικών Στοιχείων στη Σκωτία (Scottish Biometrics Commissioner Act 2020) (βλέπε https://www.legislation.gov.uk/asp/2020/8/contents) δημιουργεί τη θέση του Επιτρόπου Βιομετρικών Στοιχείων στη Σκωτία, ο οποίος πρέπει να καταρτίζει και να αναθεωρεί κώδικες ορθής πρακτικής (οι οποίοι εγκρίνονται από το Κοινοβούλιο της Σκωτίας) σχετικά με την απόκτηση, τη διατήρηση, τη χρήση και την καταστροφή βιομετρικών δεδομένων για τους σκοπούς της ποινικής δικαιοσύνης και της αστυνομίας (άρθρο 7 του νόμου του 2020 για τον Επίτροπο Βιομετρικών Στοιχείων στη Σκωτία).

οργανωτικών μέτρων. Μεταξύ αυτών περιλαμβάνεται η προστασία των δεδομένων από μη εγκεκριμένη ή παράνομη επεξεργασία και από τυχαία απώλεια, καταστροφή ή φθορά ([92]). Το άρθρο 66 του DPA 2018 ορίζει περαιτέρω ότι κάθε υπεύθυνος επεξεργασίας και κάθε εκτελών την επεξεργασία πρέπει να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα για να διασφαλίζει επίπεδο ασφάλειας κατάλληλο για τους κινδύνους που προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Σύμφωνα με τις επεξηγηματικές σημειώσεις, ο υπεύθυνος επεξεργασίας πρέπει να αξιολογεί τους κινδύνους και να εφαρμόζει κατάλληλα μέτρα ασφαλείας με βάση αυτή την αξιολόγηση, για παράδειγμα, κρυπτογράφηση ή συγκεκριμένα επίπεδα ελέγχου για το προσωπικό που επεξεργάζεται τα δεδομένα ([93]). Η αξιολόγηση πρέπει επίσης να λαμβάνει υπόψη, για παράδειγμα, τη φύση των δεδομένων που υποβάλλονται σε επεξεργασία και άλλους σχετικούς παράγοντες ή περιστάσεις που θα μπορούσαν να επηρεάσουν την ασφάλεια της επεξεργασίας.

(53) Το καθεστώς που διέπει τη συμμόρφωση με τις αρχές ασφάλειας των δεδομένων είναι παρόμοιο με εκείνο που θεσπίζεται στα άρθρα 29 έως 31 της οδηγίας (ΕΕ) 2016/680. Ειδικότερα, σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα για τα οποία έχει ευθύνη ο υπεύθυνος επεξεργασίας, σύμφωνα με το άρθρο 67 παράγραφος 1 του DPA 2018, ο υπεύθυνος επεξεργασίας πρέπει, χωρίς αδικαιολόγητη καθυστέρηση και στο μέτρο του εφικτού, εντός 72 ωρών από τη στιγμή που έλαβε γνώση της παραβίασης, να κοινοποιήσει την παραβίαση δεδομένων προσωπικού χαρακτήρα στον Επίτροπο Πληροφοριών ([94]). Η υποχρέωση κοινοποίησης δεν ισχύει όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα είναι απίθανο να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων ([95]). Ο υπεύθυνος επεξεργασίας πρέπει να τεκμηριώνει τα πραγματικά περιστατικά που σχετίζονται με οποιαδήποτε παραβίαση δεδομένων προσωπικού χαρακτήρα, τις επιπτώσεις της και τα διορθωτικά μέτρα που λαμβάνονται κατά τρόπο που να επιτρέπει στον Επίτροπο Πληροφοριών να επαληθεύσει τη συμμόρφωση με τον νόμο για την προστασία των δεδομένων ([96]). Εάν ο εκτελών την επεξεργασία αντιληφθεί παραβίαση της ασφάλειας, πρέπει να ενημερώσει τον υπεύθυνο επεξεργασίας χωρίς αδικαιολόγητη καθυστέρηση ([97]).

(54) Σύμφωνα με το άρθρο 68 παράγραφος 1 του DPA 2018, εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες προσώπων, ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει το υποκείμενο των δεδομένων σχετικά με την παραβίαση χωρίς αδικαιολόγητη καθυστέρηση ([98]). Η ειδοποίηση πρέπει να περιλαμβάνει τις ίδιες πληροφορίες που περιλαμβάνει και η κοινοποίηση στον Επίτροπο Πληροφοριών, όπως περιγράφεται στην αιτιολογική σκέψη (53). Η υποχρέωση αυτή δεν ισχύει εάν ο υπεύθυνος επεξεργασίας έχει εφαρμόσει κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, τα οποία εφαρμόστηκαν στα δεδομένα προσωπικού χαρακτήρα που επηρεάστηκαν από την παραβίαση. Δεν ισχύει επίσης εάν ο υπεύθυνος επεξεργασίας έλαβε στη συνέχεια μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανόν να προκύψει ο υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Τέλος, ο υπεύθυνος επεξεργασίας δεν υποχρεούται να ενημερώσει το υποκείμενο των δεδομένων εάν αυτό θα συνεπαγόταν δυσανάλογη προσπάθεια ([99]). Σ' αυτή την περίπτωση, οι πληροφορίες πρέπει να διατίθενται στο υποκείμενο των δεδομένων με άλλον εξίσου αποτελεσματικό τρόπο, για παράδειγμα μέσω δημόσιας ανακοίνωσης ([100]). Εάν ο υπεύθυνος επεξεργασίας δεν έχει ενημερώσει το υποκείμενο των δεδομένων για την παραβίαση, ο Επίτροπος Πληροφοριών, αφού ενημερωθεί σύμφωνα με το άρθρο 67 του DPA και αφού λάβει υπόψη την πιθανότητα η παραβίαση να οδηγήσει σε υψηλό κίνδυνο, μπορεί να απαιτήσει από τον υπεύθυνο επεξεργασίας να ενημερώσει το υποκείμενο των δεδομένων για την παραβίαση ([101]).

([92]) Σύμφωνα με τις επεξηγηματικές σημειώσεις του DPA 2018 (βλέπε υποσημείωση 45), ο υπεύθυνος επεξεργασίας οφείλει ειδικότερα: να σχεδιάζει και να οργανώνει την ασφάλειά τους ανάλογα με τη φύση των δεδομένων προσωπικού χαρακτήρα που κατέχει και ανάλογα με τη βλάβη που μπορεί να προκύψει από παραβίαση της ασφάλειας· να είναι σαφής ως προς το ποιος είναι υπεύθυνος για την ασφάλεια των πληροφοριών στο πλαίσιο του οργανισμού του· να διασφαλίζει ότι διαθέτει την κατάλληλη υλική και τεχνική ασφάλεια, με ισχυρές πολιτικές και διαδικασίες και αξιόπιστο και καλά καταρτισμένο προσωπικό· και να είναι έτοιμος να ανταποκριθεί γρήγορα και αποτελεσματικά σε κάθε παραβίαση της ασφάλειας.

([93]) Παράγραφος 221 των επεξηγηματικών σημειώσεων του DPA 2018 (βλέπε υποσημείωση 45).

([94]) Το άρθρο 67 παράγραφος 4 του DPA 2018 προβλέπει ότι η κοινοποίηση πρέπει να περιλαμβάνει περιγραφή της φύσης της παραβίασης δεδομένων προσωπικού χαρακτήρα (συμπεριλαμβανομένων, όπου είναι δυνατόν, των κατηγοριών και του κατά προσέγγιση αριθμού των οικείων υποκειμένων των δεδομένων και των κατηγοριών και του κατά προσέγγιση αριθμού των σχετικών αρχείων δεδομένων προσωπικού χαρακτήρα), το όνομα και τα στοιχεία επικοινωνίας ενός σημείου επαφής, περιγραφή των πιθανών συνεπειών της παραβίασης δεδομένων προσωπικού χαρακτήρα, και περιγραφή των μέτρων που λαμβάνονται ή προτείνεται να ληφθούν από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης των δεδομένων προσωπικού χαρακτήρα (συμπεριλαμβανομένων, κατά περίπτωση, μέτρων για τον μετριασμό των πιθανών δυσμενών συνεπειών της).

([95]) Άρθρο 67 παράγραφος 2 του DPA 2018.

([96]) Άρθρο 67 παράγραφος 6 του DPA 2018.

([97]) Άρθρο 67 παράγραφος 9 του DPA 2018.

([98]) Σύμφωνα με το άρθρο 68 παράγραφος 7 του DPA 2018, ο υπεύθυνος επεξεργασίας μπορεί να περιορίσει, εν όλω ή εν μέρει, την παροχή πληροφοριών στο υποκείμενο των δεδομένων, στον βαθμό και για όσο διάστημα ο περιορισμός, λαμβανομένων υπόψη των θεμελιωδών δικαιωμάτων και των έννομων συμφερόντων του υποκειμένου των δεδομένων, αποτελεί αναγκαίο και αναλογικό μέτρο α) για την αποφυγή της παρακώλυσης επίσημης ή νομικής έρευνας, ανάκρισης ή διαδικασίας· β) την αποφυγή της παρεμπόδισης της πρόληψης, της ανίχνευσης, της διερεύνησης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων· γ) την προστασία της δημόσιας ασφάλειας· δ) την προστασία της εθνικής ασφάλειας· ε) την προστασία των δικαιωμάτων και των ελευθεριών τρίτων.

([99]) Άρθρο 68 παράγραφος 3 του DPA 2018.

([100]) Άρθρο 68 παράγραφος 5 του DPA 2018.

([101]) Άρθρο 68 παράγραφος 6 του DPA 2018, υπό την επιφύλαξη του περιορισμού που προβλέπεται στο άρθρο 68 παράγραφος 8 του DPA 2018.

2.4.6. *Διαφάνεια*

(55) Τα υποκείμενα των δεδομένων πρέπει να ενημερώνονται για τα βασικά χαρακτηριστικά της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα τους. Αυτή η αρχή προστασίας των δεδομένων αντικατοπτρίζεται στο άρθρο 44 του DPA 2018, το οποίο, όπως και το άρθρο 13 της οδηγίας (ΕΕ) 2016/680, προβλέπει ότι ο υπεύθυνος επεξεργασίας έχει γενικό καθήκον να παρέχει στα υποκείμενα των δεδομένων πληροφορίες σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που τα αφορούν (είτε καθιστώντας τις πληροφορίες εν γένει διαθέσιμες στο κοινό είτε με οποιονδήποτε άλλον τρόπο) ([102]). Οι πληροφορίες που πρέπει να διατίθενται περιλαμβάνουν α) την ταυτότητα και τα στοιχεία επικοινωνίας του υπεύθυνου επεξεργασίας· β) κατά περίπτωση, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων· γ) τους σκοπούς για τους οποίους ο υπεύθυνος επεξεργασίας επεξεργάζεται δεδομένα προσωπικού χαρακτήρα· δ) την ύπαρξη των δικαιωμάτων των υποκειμένων των δεδομένων να υποβάλουν αίτημα στον υπεύθυνο επεξεργασίας για πρόσβαση στα δεδομένα προσωπικού χαρακτήρα, διόρθωση δεδομένων προσωπικού χαρακτήρα και διαγραφή δεδομένων προσωπικού χαρακτήρα ή για τον περιορισμό της επεξεργασίας τους· και ε) την ύπαρξη του δικαιώματος υποβολής καταγγελίας στον Επίτροπο Πληροφοριών και τα στοιχεία επικοινωνίας του Επιτρόπου ([103]).

(56) Ο υπεύθυνος επεξεργασίας πρέπει επίσης, σε ορισμένες περιπτώσεις, προκειμένου να διευκολύνει την άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων βάσει του DPA 2018 (για παράδειγμα, όταν τα δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία συλλέχθηκαν εν αγνοία του υποκειμένου των δεδομένων), να παρέχει στο υποκείμενο των δεδομένων πληροφορίες σχετικά α) με τη νομική βάση της επεξεργασίας· β) πληροφορίες σχετικά με το χρονικό διάστημα αποθήκευσης των δεδομένων προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, σχετικά με τα κριτήρια που καθορίζουν το εν λόγω διάστημα· γ) όπου συντρέχει περίπτωση, πληροφορίες για τις κατηγορίες αποδεκτών των δεδομένων προσωπικού χαρακτήρα (μεταξύ άλλων αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς)· δ) περαιτέρω πληροφορίες που είναι απαραίτητες για να καταστεί δυνατή η άσκηση των δικαιωμάτων του υποκειμένου των δεδομένων σύμφωνα με το μέρος 3 του DPA 2018 ([104]).

2.4.7. *Ατομικά δικαιώματα*

(57) Τα υποκείμενα των δεδομένων πρέπει να διαθέτουν ορισμένα εκτελεστά δικαιώματα. Το μέρος 3 κεφάλαιο 3 του DPA 2018 παρέχει στα φυσικά πρόσωπα δικαιώματα πρόσβασης, διόρθωσης και διαγραφής, καθώς και περιορισμού ([105]), τα οποία είναι συγκρίσιμα με εκείνα που προβλέπονται στο κεφάλαιο 3της οδηγίας (ΕΕ) 2016/680.

(58) Το δικαίωμα πρόσβασης καθορίζεται στο άρθρο 45 του DPA 2018. Πρώτον, ένα πρόσωπο δικαιούται να λάβει επιβεβαίωση από τον υπεύθυνο επεξεργασίας για το αν τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υποβάλλονται σε επεξεργασία ή όχι ([106]). Δεύτερον, όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία, το υποκείμενο των δεδομένων έχει δικαίωμα πρόσβασης στα εν λόγω δεδομένα καθώς και δικαίωμα να λάβει τις ακόλουθες πληροφορίες σχετικά με την επεξεργασία: α) τους σκοπούς και τις νομικές βάσεις της επεξεργασίας· β) τις κατηγορίες των σχετικών δεδομένων· γ) τον αποδέκτη στον οποίο έχουν κοινολογηθεί τα δεδομένα· δ) το χρονικό διάστημα αποθήκευσης των δεδομένων προσωπικού χαρακτήρα· ε) την ύπαρξη δικαιώματος του υποκειμένου των δεδομένων για διόρθωση και διαγραφή δεδομένων προσωπικού χαρακτήρα· στ) το δικαίωμα υποβολής καταγγελίας· και ζ) οποιαδήποτε πληροφορία σχετικά με την προέλευση των εν λόγω δεδομένων προσωπικού χαρακτήρα ([107]).

(59) Σύμφωνα με το άρθρο 46 του DPA 2018, το υποκείμενο των δεδομένων έχει το δικαίωμα να απαιτήσει από τον υπεύθυνο επεξεργασίας να διορθώσει ανακριβή δεδομένα προσωπικού χαρακτήρα που το αφορούν. Ο υπεύθυνος επεξεργασίας πρέπει να διορθώσει (ή σε περίπτωση που τα δεδομένα είναι ανακριβή επειδή είναι ελλιπή, να συμπληρώσει) τα δεδομένα χωρίς αδικαιολόγητη καθυστέρηση. Εάν τα δεδομένα προσωπικού χαρακτήρα πρέπει να διατηρηθούν για αποδεικτικούς σκοπούς, ο υπεύθυνος επεξεργασίας πρέπει (αντί να διορθώνει τα δεδομένα προσωπικού χαρακτήρα) να περιορίζει την επεξεργασία τους ([108]).

([102]) Στον οδηγό για την επεξεργασία στον τομέα της επιβολής του νόμου (Guide to Law Enforcement Processing) παρέχεται το ακόλουθο παράδειγμα: «Έχετε μια γενική δήλωση περί ιδιωτικότητας στον ιστότοπό σας, η οποία καλύπτει βασικές πληροφορίες σχετικά με τον οργανισμό, τον σκοπό για τον οποίο επεξεργάζεστε δεδομένα προσωπικού χαρακτήρα, τα δικαιώματα του υποκειμένου των δεδομένων και το δικαίωμά του να υποβάλει καταγγελία στον Επίτροπο Πληροφοριών. Έχετε λάβει πληροφορίες ότι ένα πρόσωπο ήταν παρόν κατά τη διάπραξη εγκλήματος. Κατά την πρώτη συνέντευξη με το πρόσωπο αυτό, πρέπει να παράσχετε τις γενικές πληροφορίες, καθώς και τις περαιτέρω συνοδευτικές πληροφορίες, ώστε να το πρόσωπο να έχει τη δυνατότητα να ασκήσει τα δικαιώματά του. Μπορείτε να περιορίσετε τις πληροφορίες δίκαιης επεξεργασίας που παρέχετε μόνο εάν αυτές πρόκειται να επηρεάσουν αρνητικά την έρευνα που διεξάγετε» (Guide to Law Enforcement Processing, "What information should we supply to an individual?", διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) Στον οδηγό για την επεξεργασία στον τομέα της επιβολής του νόμου αναφέρεται ότι οι πληροφορίες που παρέχονται σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να είναι συνοπτικές, κατανοητές και εύκολα προσβάσιμες· να είναι γραμμένες σε σαφή και απλή γλώσσα που θα προσαρμόζεται στις ανάγκες των ευάλωτων προσώπων, όπως παιδιά· και δωρεάν (Guide to Law Enforcement Processing, "How should we provide this information?", διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1).

([104]) Άρθρο 44 παράγραφος 2 του DPA 2018.

([105]) Για λεπτομερή ανάλυση των δικαιωμάτων των υποκειμένων, βλέπε: Guide to Law Enforcement Processing, ενότητα σχετικά με τα ατομικά δικαιώματα, που διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/.

([106]) Άρθρο 45 παράγραφος 1 του DPA 2018.

([107]) Άρθρο 45 παράγραφος 2 του DPA 2018.

([108]) Άρθρο 46 παράγραφος 4 του DPA 2018.

(60) Το άρθρο 47 του DPA 2018 παρέχει στα φυσικά πρόσωπα το δικαίωμα διαγραφής και περιορισμού της επεξεργασίας. Ο υπεύθυνος επεξεργασίας πρέπει ([109]) να διαγράφει τα δεδομένα προσωπικού χαρακτήρα χωρίς αδικαιολόγητη καθυστέρηση όταν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα θα παρέβαινε οποιαδήποτε από τις αρχές προστασίας των δεδομένων, τους νομικούς λόγους της επεξεργασίας ή τις εγγυήσεις που σχετίζονται με την αρχειοθέτηση και την επεξεργασία ευαίσθητων δεδομένων. Ο υπεύθυνος επεξεργασίας πρέπει επίσης να διαγράψει τα δεδομένα εάν υπέχει σχετική νομική υποχρέωση. Εάν τα δεδομένα προσωπικού χαρακτήρα πρέπει να διατηρηθούν για αποδεικτικούς σκοπούς, ο υπεύθυνος επεξεργασίας πρέπει να περιορίζει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα (αντί να τα διαγράφει) ([110]). Ο υπεύθυνος επεξεργασίας πρέπει να περιορίζει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα εάν το υποκείμενο των δεδομένων αμφισβητεί την ακρίβεια των δεδομένων προσωπικού χαρακτήρα, αλλά δεν είναι δυνατόν να εξακριβωθεί αν αυτά είναι ακριβή ή όχι ([111]).

(61) Όταν το υποκείμενο των δεδομένων ζητεί τη διόρθωση ή τη διαγραφή δεδομένων προσωπικού χαρακτήρα ή τον περιορισμό της επεξεργασίας τους, ο υπεύθυνος επεξεργασίας πρέπει να ενημερώνει γραπτώς το υποκείμενο των δεδομένων σχετικά με το αν το αίτημα έγινε δεκτό και σε περίπτωση που αυτό απορρίπτεται, να ενημερώνει το υποκείμενο των δεδομένων για τους λόγους της απόρριψης και για τα διαθέσιμα ένδικα μέσα (δικαίωμα του υποκειμένου των δεδομένων να υποβάλει αίτημα στον Επίτροπο Πληροφοριών για τη διερεύνηση της νομιμότητας του περιορισμού, δικαίωμα υποβολής καταγγελίας στον Επίτροπο Πληροφοριών και δικαίωμα υποβολής αίτησης σε δικαστήριο για έκδοση εντολής συμμόρφωσης) ([112]).

(62) Όταν ο υπεύθυνος επεξεργασίας διορθώνει δεδομένα προσωπικού χαρακτήρα που έχει λάβει από άλλη αρμόδια αρχή, πρέπει να ενημερώνει την άλλη αρχή ([113]). Όταν ο υπεύθυνος επεξεργασίας διορθώνει, διαγράφει ή περιορίζει την επεξεργασία δεδομένων προσωπικού χαρακτήρα τα οποία έχουν κοινολογηθεί από τον υπεύθυνο επεξεργασίας, πρέπει να ενημερώνει τους αποδέκτες, οι οποίοι με τη σειρά τους πρέπει να διορθώσουν, να διαγράψουν ή να περιορίσουν την επεξεργασία των δεδομένων προσωπικού χαρακτήρα (στο μέτρο που φέρουν ευθύνη γι' αυτά) ([114]).

(63) Επιπλέον, το υποκείμενο των δεδομένων έχει το δικαίωμα να ενημερώνεται χωρίς αδικαιολόγητη καθυστέρηση από τον υπεύθυνο επεξεργασίας σχετικά με παραβίαση δεδομένων προσωπικού χαρακτήρα, όταν αυτή ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες προσώπων ([115]).

(64) Όσον αφορά όλα τα δικαιώματα του υποκειμένου των δεδομένων και όπως προβλέπεται και στο άρθρο 12 της οδηγίας (ΕΕ) 2016/680, ο υπεύθυνος επεξεργασίας έχει την υποχρέωση να διασφαλίζει ότι παρέχει στο υποκείμενο των δεδομένων κάθε πληροφορία σε συνοπτική, κατανοητή και ευκόλως προσβάσιμη μορφή ([116]) και, όπου είναι δυνατόν, με την ίδια μορφή που υποβλήθηκε η αίτηση ([117]). Ο υπεύθυνος επεξεργασίας πρέπει να συμμορφώνεται με το αίτημα του υποκειμένου των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση ή σε κάθε περίπτωση, καταρχήν, πριν από τη λήξη της προθεσμίας ενός μηνός από την υποβολή του αιτήματος ([118]). Όταν ο υπεύθυνος επεξεργασίας έχει εύλογες αμφιβολίες σχετικά με την ταυτότητα ενός προσώπου, μπορεί να ζητήσει πρόσθετες πληροφορίες και να καθυστερήσει τη διεκπεραίωση του αιτήματος έως ότου εξακριβωθεί η ταυτότητα του εν λόγω προσώπου. Ο υπεύθυνος επεξεργασίας μπορεί να απαιτήσει την καταβολή εύλογου τέλους ή να αρνηθεί να απαντήσει στο αίτημα όταν κρίνει ότι το αίτημα είναι προδήλως αβάσιμο ([119]). Το ICO έχει παράσχει καθοδήγηση σχετικά με το πότε ένα αίτημα θεωρείται προδήλως αβάσιμο ή υπερβολικό και πότε μπορεί να ζητηθεί η καταβολή τέλους ([120]).

(65) Επιπλέον, σύμφωνα με το άρθρο 53 παράγραφος 4 του DPA 2018, ο ανώτερος υπουργός μπορεί να ορίσει το ανώτατο ποσό του τέλους, βάσει κανονισμών.

([109]) Το υποκείμενο των δεδομένων μπορεί να ζητήσει από τον υπεύθυνο επεξεργασίας να διαγράψει δεδομένα προσωπικού χαρακτήρα ή να περιορίσει την επεξεργασία τους (αλλά τα καθήκοντα του υπευθύνου επεξεργασίας να διαγράφει δεδομένα προσωπικού χαρακτήρα ή να περιορίζει την επεξεργασία τους ισχύουν ανεξάρτητα από το αν υποβάλλεται τέτοιο αίτημα ή όχι).

([110]) Άρθρο 46 παράγραφος 4 και άρθρο 47 παράγραφος 2 του DPA 2018.

([111]) Άρθρο 47 παράγραφος 3 του DPA 2018.

([112]) Άρθρο 48 παράγραφος 1 του DPA 2018.

([113]) Άρθρο 48 παράγραφος 7 του DPA 2018.

([114]) Άρθρο 48 παράγραφος 9 του DPA 2018.

([115]) Άρθρο 68 του DPA 2018.

([116]) Άρθρο 52 παράγραφος 1 του DPA 2018.

([117]) Άρθρο 52 παράγραφος 3 του DPA 2018.

([118]) Το άρθρο 54 του DPA 2018 ορίζει την έννοια της «εφαρμοστέας χρονικής περιόδου», η οποία νοείται ως διάστημα ενός μηνός ή μεγαλύτερο διάστημα που μπορεί να ορίζεται σε κανονισμούς, αρχής γενομένης από τη σχετική χρονική στιγμή [όταν ο υπεύθυνος επεξεργασίας παραλαμβάνει το εν λόγω αίτημα· όταν ο υπεύθυνος επεξεργασίας λαμβάνει τις πληροφορίες (εφόσον υπάρχουν) που ζητούνται σε σχέση με αίτημα βάσει του άρθρου 52 παράγραφος 4 του DPA· ή όταν καταβληθεί το τέλος (εάν υπάρχει) που χρεώνεται σε σχέση με το αίτημα βάσει του άρθρου 53 του DPA].

([119]) Άρθρο 53 παράγραφος 1 του DPA 2018.

([120]) Σύμφωνα με τις οδηγίες του ICO, ο υπεύθυνος επεξεργασίας μπορεί να αποφασίσει να επιβάλει την καταβολή τέλους στο υποκείμενο των δεδομένων εάν το αίτημά του είναι προδήλως αβάσιμο ή υπερβολικό, αλλά παρ' όλα αυτά επιλέγει να απαντήσει σ' αυτό. Το τέλος πρέπει να είναι εύλογο και ικανό να δικαιολογήσει το κόστος. Guide to Law Enforcement Processing "Manifestly unfounded and excessive requests", διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

2.4.7.1. Περιορισμοί των δικαιωμάτων του υποκειμένου των δεδομένων και υποχρεώσεις διαφάνειας

(66) Η αρμόδια αρχή μπορεί, υπό ορισμένες προϋποθέσεις, να περιορίσει ορισμένα δικαιώματα του υποκειμένου των δεδομένων: Το δικαίωμα πρόσβασης ([121]), πληροφόρησης ([122]), ενημέρωσης σχετικά με παραβίαση δεδομένων προσωπικού χαρακτήρα ([123]) και ενημέρωσης σχετικά με τον λόγο απόρριψης αιτήματος διόρθωσης ή διαγραφής ([124]). Αντίστοιχα με το καθεστώς που περιλαμβάνεται στο κεφάλαιο III της οδηγίας (ΕΕ) 2016/680, η αρμόδια αρχή μπορεί να εφαρμόσει τον περιορισμό όταν, δεδομένων των θεμελιωδών δικαιωμάτων και των έννομων συμφερόντων του υποκειμένου των δεδομένων, αυτός είναι αναγκαίος και αναλογικός για: α) την αποφυγή της παρακώλυσης επίσημης ή νομικής έρευνας, ανάκρισης ή διαδικασίας· β) την αποφυγή της παρεμπόδισης της πρόληψης, της ανίχνευσης, της διερεύνησης ή της δίωξης ποινικών αδικημάτων ή της εκτέλεσης ποινικών κυρώσεων· γ) την προστασία της δημόσιας ασφάλειας· δ) την προστασία της εθνικής ασφάλειας· ε) την προστασία των δικαιωμάτων και των ελευθεριών τρίτων.

(67) Το ICO έχει παράσχει καθοδήγηση σχετικά με την εφαρμογή αυτών των περιορισμών. Σύμφωνα με την καθοδήγηση αυτή, οι υπεύθυνοι επεξεργασίας πρέπει να διενεργούν ανάλυση κατά περίπτωση για να σταθμίζουν τα δικαιώματα του προσώπου έναντι της ζημίας που θα προκαλούσε η κοινολόγηση των δεδομένων. Συγκεκριμένα, πρέπει να αιτιολογούν κάθε περιορισμό που εφαρμόζεται ως αναγκαίος και αναλογικός και μπορούν να περιορίζουν τα προβλεπόμενα μόνο εάν θα θίγονταν οι προαναφερθέντες σκοποί ([125]).

(68) Υπάρχουν επίσης ορισμένα άλλα έγγραφα καθοδήγησης που εκδίδονται από τις αρμόδιες αρχές και παρέχουν αναλυτικές πληροφορίες σχετικά με όλες τις πτυχές της νομοθεσίας για την προστασία των δεδομένων, μεταξύ άλλων σχετικά με την εφαρμογή περιορισμών στα δικαιώματα των υποκειμένων των δεδομένων ([126]). Για παράδειγμα, σε σχέση με το άρθρο 45 παράγραφος 4, το εγχειρίδιο προστασίας δεδομένων του Εθνικού Συμβουλίου Αρχηγών της Αστυνομίας αναφέρει ότι: «Είναι σημαντικό να σημειωθεί ότι οι περιορισμοί μπορούν να εφαρμόζονται μόνο στον βαθμό που είναι αναγκαίο και μπορούν να εφαρμόζονται μόνο για όσο διάστημα είναι αναγκαίο. Κατά συνέπεια, δεν επιτρέπεται η γενική εφαρμογή του περιορισμού σε όλα τα δεδομένα προσωπικού χαρακτήρα του αιτούντος ή η μόνιμη εφαρμογή του περιορισμού. Όσον αφορά τη δεύτερη περίπτωση, συχνά τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται εν αγνοία του υποκειμένου των δεδομένων που είναι ύποπτο στο πλαίσιο έρευνας πρέπει να προστατεύονται αρχικά από την κοινολόγησή τους σ' αυτό, ώστε να αποφευχθεί το ενδεχόμενο να θιγεί η έρευνα όσο βρίσκεται σε εξέλιξη, αλλά σε μεταγενέστερη ημερομηνία η κοινολόγηση δεν θα δημιουργούσε πρόβλημα εάν τα δεδομένα προσωπικού χαρακτήρα είχαν κοινολογηθεί στο πρόσωπο κατά τη διάρκεια της ανάκρισης. Οι αστυνομικές δυνάμεις πρέπει να θεσπίζουν διαδικασίες που διασφαλίζουν ότι οι περιορισμοί εφαρμόζονται μόνο στον βαθμό που απαιτείται και ισχύουν μόνο για την αναγκαία διάρκεια» ([127]). Ο οδηγός αυτός παρέχει επίσης παραδείγματα περιπτώσεων στις οποίες είναι πιθανή η εφαρμογή καθενός από τους περιορισμούς ([128]).

(69) Επιπλέον, όσον αφορά τη δυνατότητα περιορισμού οποιουδήποτε από τα προαναφερόμενα δικαιώματα για την προστασία της «εθνικής ασφάλειας», ο υπεύθυνος επεξεργασίας μπορεί να υποβάλει αίτηση για πιστοποιητικό υπογεγραμμένο από υπουργό ή από τον Γενικό Εισαγγελέα (ή τον Γενικό Εισαγγελέα της Σκωτίας) που πιστοποιεί ότι ο περιορισμός των εν λόγω δικαιωμάτων αποτελεί αναγκαίο και αναλογικό μέτρο για την προστασία της εθνικής ασφάλειας ([129]). Η κυβέρνηση του Ηνωμένου Βασιλείου έχει εκδώσει οδηγίες σχετικά με τα πιστοποιητικά εθνικής ασφάλειας δυνάμει του DPA 2018 στις οποίες επισημαίνεται κυρίως ότι κάθε περιορισμός των δικαιωμάτων των υποκειμένων των δεδομένων για τη διαφύλαξη της εθνικής ασφάλειας πρέπει να είναι αναλογικός και αναγκαίος ([130]) (για περισσότερες λεπτομέρειες σχετικά με τα πιστοποιητικά εθνικής ασφάλειας, βλέπε αιτιολογικές σκέψεις (131) έως (134)).

([121]) Άρθρο 45 παράγραφος 4 του DPA 2018.
([122]) Άρθρο 44 παράγραφος 4 του DPA 2018.
([123]) Άρθρο 68 παράγραφος 7 του DPA 2018.
([124]) Άρθρο 48 παράγραφος 3 του DPA 2018.
([125]) Βλέπε για παράδειγμα, Guide to Law Enforcement Processing, ενότητα σχετικά με το δικαίωμα πρόσβασης, που διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8.
([126]) Βλέπε, για παράδειγμα, Data Protection Manual for Police Data Protection Professional, το οποίο έχει εκδοθεί από το Εθνικό Συμβούλιο Αρχηγών της Αστυνομίας (βλέπε υποσημείωση 27) ή τον οδηγό που παρέχεται από την υπηρεσία σοβαρών περιπτώσεων απάτης, ο οποίος διατίθεται στον ακόλουθο σύνδεσμο: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/.
([127]) Εγχειρίδιο προστασίας δεδομένων του Εθνικού Συμβουλίου Αρχηγών της Αστυνομίας, σ. 140 (βλέπε υποσημείωση 27).
([128]) Το εγχειρίδιο προστασίας δεδομένων του Εθνικού Συμβουλίου Αρχηγών της Αστυνομίας προβλέπει ότι «η αποφυγή της παρακώλυσης επίσημης ή νομικής έρευνας, ανάκρισης ή διαδικασίας» είναι πιθανό να αφορά δεδομένα προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία για έρευνες, δικαστικές υποθέσεις οικογενειακών διαφορών, εσωτερικές πειθαρχικές έρευνες μη ποινικής φύσης και έρευνες όπως η ανεξάρτητη έρευνα για τη σεξουαλική κακοποίηση παιδιών· ενώ παράλληλα «η προστασία των δικαιωμάτων και των ελευθεριών τρίτων» αφορά δεδομένα προσωπικού χαρακτήρα που αφορούν και άλλα φυσικά πρόσωπα, καθώς και τον αιτούντα» (Εγχειρίδιο προστασίας του Εθνικού Συμβουλίου Αρχηγών της Αστυνομίας, σ. 140, βλέπε υποσημείωση 27).
([129]) Άρθρο 79 του DPA 2018.
([130]) UK Government Guidance on National Security Certificates, διατίθεται στον ακόλουθο σύνδεσμο: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

(70) Επιπλέον, όταν εφαρμόζεται περιορισμός σε δικαίωμα υποκειμένου των δεδομένων, η αρμόδια αρχή πρέπει να ενημερώνει το υποκείμενο των δεδομένων χωρίς αδικαιολόγητη καθυστέρηση ότι τα δικαιώματά του έχουν περιοριστεί, σχετικά με τους λόγους του περιορισμού και τα διαθέσιμα ένδικα μέσα, εκτός εάν η παροχή των εν λόγω πληροφοριών θα υπονόμευε τον λόγο εφαρμογής του περιορισμού ([131]). Ως περαιτέρω διασφάλιση κατά της κατάχρησης των περιορισμών, ο υπεύθυνος επεξεργασίας πρέπει να καταγράφει τους λόγους περιορισμού της πληροφόρησης και να θέτει το αρχείο στη διάθεση του Επιτρόπου Πληροφοριών εφόσον του ζητηθεί ([132]).

(71) Εάν ο υπεύθυνος επεξεργασίας αρνηθεί να παράσχει πρόσθετες πληροφορίες σχετικά με τη διαφάνεια, ή αρνηθεί την πρόσβαση, ή απορρίψει αίτημα διόρθωσης, διαγραφής ή περιορισμού της επεξεργασίας, το πρόσωπο μπορεί να ζητήσει από τον Επίτροπο Πληροφοριών να διερευνήσει αν ο υπεύθυνος επεξεργασίας προέβη σε νόμιμη χρήση του περιορισμού ([133]). Το ενδιαφερόμενο πρόσωπο μπορεί επίσης να υποβάλει καταγγελία στον Επίτροπο Πληροφοριών ή να υποβάλει αίτηση σε δικαστήριο ώστε να διατάξει τον υπεύθυνο επεξεργασίας να συμμορφωθεί με το αίτημα ([134]).

2.4.7.2. Αυτοματοποιημένη λήψη αποφάσεων

(72) Τα άρθρα 49 και 50 του DPA 2018 καλύπτουν αντίστοιχα τα δικαιώματα που σχετίζονται την αυτοματοποιημένη λήψη αποφάσεων και τις εγγυήσεις που πρέπει να εφαρμόζονται ([135]). Όπως και βάσει του άρθρου 11 της οδηγίας (ΕΕ) 2016/680, ο υπεύθυνος επεξεργασίας μπορεί να λάβει σημαντική απόφαση βασιζόμενος αποκλειστικά στην αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα μόνον εφόσον αυτή απαιτείται ή επιτρέπεται από τον νόμο ([136]). Η απόφαση είναι σημαντική εάν παράγει δυσμενή έννομα αποτελέσματα για το υποκείμενο των δεδομένων ή επηρεάζει σε σημαντικό βαθμό το υποκείμενο των δεδομένων ([137]).

(73) Όταν ο υπεύθυνος επεξεργασίας υποχρεούται ή εξουσιοδοτείται από τον νόμο να λάβει σημαντική απόφαση, το άρθρο 50 του DPA 2018 ορίζει τις εγγυήσεις που θα ισχύουν για μια τέτοια απόφαση (η οποία ορίζεται ως «σημαντική απόφαση που πληροί τις προϋποθέσεις»). Ο υπεύθυνος επεξεργασίας πρέπει, αμέσως μόλις αυτό είναι ευλόγως εφικτό, να γνωστοποιήσει στο υποκείμενο των δεδομένων ότι ελήφθη η σχετική απόφαση. Στη συνέχεια, το υποκείμενο των δεδομένων μπορεί, εντός ενός μηνός, να ζητήσει από τον υπεύθυνο επεξεργασίας να επανεξετάσει την απόφαση ή να λάβει νέα απόφαση που δεν βασίζεται αποκλειστικά σε αυτοματοποιημένη επεξεργασία. Ο υπεύθυνος επεξεργασίας πρέπει να εξετάσει το αίτημα και να ενημερώσει το υποκείμενο των δεδομένων για το αποτέλεσμα της εξέτασης αυτής. Ο DPA 2018 παρέχει στον ανώτερο υπουργό την εξουσία να θεσπίζει κανονισμούς για πρόσθετες εγγυήσεις ([138]). Δεν έχουν εκδοθεί ακόμη τέτοιοι κανονισμοί.

2.4.8. *Περαιτέρω διαβιβάσεις*

(74) Το επίπεδο προστασίας που παρέχεται στα δεδομένα προσωπικού χαρακτήρα που διαβιβάζονται από αρχή επιβολής του νόμου κράτους μέλους σε αρχή επιβολής του νόμου του Ηνωμένου Βασιλείου δεν πρέπει να υποβαθμίζεται από την περαιτέρω διαβίβαση των εν λόγω δεδομένων σε αποδέκτες σε τρίτη χώρα. Αυτές οι «περαιτέρω διαβιβάσεις», οι οποίες από τη σκοπιά αρχής επιβολής του νόμου του Ηνωμένου Βασιλείου συνιστούν διεθνείς διαβιβάσεις από το Ηνωμένο Βασίλειο, θα πρέπει να επιτρέπονται μόνον όταν ο περαιτέρω αποδέκτης εκτός του Ηνωμένου Βασιλείου υπόκειται επίσης σε κανόνες που διασφαλίζουν ανάλογο επίπεδο προστασίας με εκείνο που εγγυάται η έννομη τάξη του Ηνωμένου Βασιλείου.

([131]) Άρθρο 44 παράγραφοι 5 και 6· άρθρο 45 παράγραφοι 5 και 6· άρθρο 48 παράγραφος 4 του DPA 2018.

([132]) Άρθρο 44 παράγραφος 7· άρθρο 45 παράγραφος 7· άρθρο 48 παράγραφος 6 του DPA 2018.

([133]) Άρθρο 51 του DPA 2018.

([134]) Άρθρο 167 του DPA 2018.

([135]) Όσον αφορά το πεδίο εφαρμογής της αυτοματοποιημένης επεξεργασίας, στις επεξηγηματικές σημειώσεις του DPA 2018 αναφέρεται ότι: «αυτές οι διατάξεις αφορούν την πλήρως αυτοματοποιημένη λήψη αποφάσεων και όχι την αυτοματοποιημένη επεξεργασία. Αυτοματοποιημένη επεξεργασία (συμπεριλαμβανομένης της κατάρτισης προφίλ) υφίσταται όταν μια πράξη εκτελείται στα δεδομένα χωρίς να απαιτείται ανθρώπινη παρέμβαση. Χρησιμοποιείται τακτικά στον τομέα της επιβολής του νόμου για το φιλτράρισμα μεγάλων συνόλων δεδομένων, ώστε αυτά να καταστούν διαχειρίσιμα και να μπορούν να χρησιμοποιηθούν από άνθρωπο. Η αυτοματοποιημένη λήψη αποφάσεων είναι μια μορφή αυτοματοποιημένης επεξεργασίας και απαιτεί η τελική απόφαση να λαμβάνεται χωρίς ανθρώπινη παρέμβαση». (Επεξηγηματικές σημειώσεις του DPA, παράγραφος 204, βλέπε υποσημείωση 45).

([136]) Επιπλέον της προστασίας που προβλέπεται στον DPA, υπάρχουν και άλλοι νομοθετικοί περιορισμοί στο νομικό πλαίσιο του Ηνωμένου Βασιλείου, οι οποίοι εφαρμόζονται τις υπηρεσίες επιβολής του νόμου και αποτρέπουν την αυτοματοποιημένη επεξεργασία (συμπεριλαμβανομένης της κατάρτισης προφίλ) που οδηγεί σε παράνομες διακρίσεις. Ο νόμος του 1998 για τα ανθρώπινα δικαιώματα ενσωματώνει στο δίκαιο του Ηνωμένου Βασιλείου τα δικαιώματα που απορρέουν από την ΕΣΔΑ, συμπεριλαμβανομένου του δικαιώματος της απαγόρευσης των διακρίσεων που κατοχυρώνεται στο άρθρο 14 της σύμβασης. Ομοίως, ο νόμος του 2010 για την ισότητα απαγορεύει τις διακρίσεις σε βάρος ατόμων με προστατευόμενα χαρακτηριστικά (στα οποία συμπεριλαμβάνονται το φύλο, η φυλή, η αναπηρία κ.λπ.).

([137]) Άρθρο 49 παράγραφος 2 του DPA 2018.

([138]) Άρθρο 50 παράγραφος 4 του DPA 2018.

(75) Το καθεστώς του Ηνωμένου Βασιλείου σχετικά με τις διεθνείς διαβιβάσεις ρυθμίζεται από το μέρος 3 κεφάλαιο 5 του DPA 2018 ([139]) και αντικατοπτρίζει την προσέγγιση που ακολουθείται στο κεφάλαιο V της οδηγίας (ΕΕ) 2016/680. Ειδικότερα, για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα, η αρμόδια αρχή πρέπει να πληροί τρεις προϋποθέσεις: α) η διαβίβαση πρέπει να είναι αναγκαία για σκοπούς επιβολής του νόμου· β) η διαβίβαση πρέπει να βασίζεται: i) σε κανονισμό περί επάρκειας όσον αφορά την τρίτη χώρα, ii) εάν δεν βασίζεται σε κανονισμό περί επάρκειας, στην ύπαρξη κατάλληλων εγγυήσεων, ή iii) εάν δεν βασίζεται σε απόφαση περί επάρκειας ή σε κατάλληλες εγγυήσεις, πρέπει να βασίζεται σε ειδικές περιστάσεις· και γ) ο αποδέκτης της διαβίβασης πρέπει να είναι: i) οικεία αρχή (δηλαδή το ισοδύναμο αρμόδιας αρχής) σε τρίτη χώρα· ii) «σχετικός διεθνής οργανισμός», π.χ. διεθνής φορέας που εκτελεί καθήκοντα που αντιστοιχούν σε οποιονδήποτε από τους σκοπούς επιβολής του νόμου· ή iii) πρόσωπο που δεν είναι οικεία αρχή, αλλά μόνον όταν η διαβίβαση είναι απολύτως αναγκαία για την εκπλήρωση ενός από τους σκοπούς επιβολής του νόμου· δεν υπάρχουν θεμελιώδη δικαιώματα και ελευθερίες του σχετικού υποκειμένου των δεδομένων που να υπερισχύουν του δημόσιου συμφέροντος το οποίο απαιτεί τη διαβίβαση· η διαβίβαση των δεδομένων προσωπικού χαρακτήρα σε οικεία αρχή στην τρίτη χώρα θα ήταν αναποτελεσματική ή ακατάλληλη· και ο αποδέκτης είναι ενήμερος για τους σκοπούς για τους οποίους τα δεδομένα μπορεί να υποβληθούν σε επεξεργασία ([140]).

(76) Ο ανώτερος υπουργός εκδίδει κανονισμούς περί επάρκειας όσον αφορά τρίτη χώρα, έδαφος ή τομέα εντός τρίτης χώρας, διεθνή οργανισμό, ή περιγραφή ([141]) της εν λόγω χώρας, εδάφους, τομέα ή οργανισμού. Όσον αφορά το πρότυπο που πρέπει να τηρείται, ο ανώτερος υπουργός πρέπει να αξιολογεί αν το εν λόγω έδαφος/τομέας/οργανισμός διασφαλίζει επαρκές επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα. Το άρθρο 74Α παράγραφος 4 του DPA 2018 ορίζει ότι, για τον σκοπό αυτόν, ο ανώτερος υπουργός πρέπει να εξετάζει ορισμένα στοιχεία που αποτυπώνουν εκείνα που απαριθμούνται στο άρθρο 36 της οδηγίας (ΕΕ) 2016/680 ([142]). Στο πλαίσιο αυτό, από τη λήξη της μεταβατικής περιόδου, το μέρος 3 του DPA 2018 αποτελεί «εσωτερική νομοθεσία που προέρχεται από την ΕΕ» η οποία, όπως εξηγείται, θα ερμηνεύεται από τα δικαστήρια του Ηνωμένου Βασιλείου σύμφωνα με τη σχετική νομολογία του Δικαστηρίου της ΕΕ η οποία χρονολογείται πριν από την αποχώρηση του Ηνωμένου Βασιλείου από την Ένωση, και τις γενικές αρχές του ενωσιακού δικαίου, όπως ίσχυαν αμέσως πριν από τη λήξη της μεταβατικής περιόδου. Μεταξύ αυτών, περιλαμβάνεται το πρότυπο της «κατ' ουσίαν ισοδυναμίας» που θα εφαρμόζεται ως εκ τούτου στις εκτιμήσεις επάρκειας που διενεργούνται από τις αρχές του Ηνωμένου Βασιλείου.

(77) Όσον αφορά τη διαδικασία, οι κανονισμοί υπόκεινται στις «γενικές» διαδικαστικές απαιτήσεις που προβλέπονται στο άρθρο 182 του DPA 2018. Στο πλαίσιο της διαδικασίας αυτής, ο ανώτερος υπουργός πρέπει να συμβουλεύεται τον

([139]) Το νέο αυτό πλαίσιο τέθηκε σε εφαρμογή κατά τη λήξη της μεταβατικής περιόδου, συμπεριλαμβανομένης της εξουσίας του ανώτερου υπουργού να εκδίδει κανονισμούς περί επάρκειας. Ωστόσο, οι κανονισμοί DPPEC (ειδικότερα, οι παράγραφοι 10-12 του παραρτήματος 21 τις οποίες εισάγουν οι εν λόγω κανονισμοί στον DPA 2018) προβλέπουν ότι ορισμένες διαβιβάσεις δεδομένων προσωπικού χαρακτήρα κατά τη λήξη της μεταβατικής περιόδου και μετά τη λήξη αυτής αντιμετωπίζονται ωσάν να βασίζονται σε κανονισμούς περί επάρκειας. Οι εν λόγω διαβιβάσεις περιλαμβάνουν διαβιβάσεις σε τρίτες χώρες που αποτελούν αντικείμενο ενωσιακής απόφασης επάρκειας κατά τη λήξη της μεταβατικής περιόδου, και σε κράτη μέλη της ΕΕ, σε κράτη της ΕΖΕΣ και στο έδαφος του Γιβραλτάρ δυνάμει της εφαρμογής της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου στην επεξεργασία δεδομένων για σκοπούς επιβολής του νόμου [τα κράτη της ΕΖΕΣ εφαρμόζουν την οδηγία (ΕΕ) 2016/680 ως αποτέλεσμα των υποχρεώσεών τους δυνάμει του κεκτημένου του Σένγκεν]. Αυτό σημαίνει ότι κατά τη λήξη της μεταβατικής περιόδου οι διαβιβάσεις προς τις χώρες αυτές μπορούν να συνεχιστούν όπως και πριν από την έξοδο από την ΕΕ. Μετά τη λήξη της μεταβατικής περιόδου, ο υπουργός πρέπει να προβεί σε επανεξέταση των διαπιστώσεων επάρκειας εντός 4 ετών.

([140]) Άρθρα 73 και 77 του DPA 2018.

([141]) Οι αρχές του Ηνωμένου Βασιλείου εξήγησαν ότι η περιγραφή μιας χώρας ή ενός διεθνούς οργανισμού αναφέρεται σε μια κατάσταση στην οποία θα ήταν αναγκαίο να πραγματοποιηθεί ειδικός και μερικός προσδιορισμός της επάρκειας με εστιασμένους περιορισμούς (για παράδειγμα, κανονισμός περί επάρκειας σε σχέση με συγκεκριμένο μόνο είδος διαβιβάσεων δεδομένων).

([142]) Βλέπε άρθρο 74Α παράγραφος 4 του DPA 2018 που προβλέπει ότι, κατά την αξιολόγηση της επάρκειας του επιπέδου προστασίας «ο ανώτερος υπουργός πρέπει, ειδικότερα, να λαμβάνει υπόψη α) το κράτος δικαίου, τον σεβασμό των ανθρώπινων δικαιωμάτων και των θεμελιωδών ελευθεριών, τη σχετική νομοθεσία, τόσο γενική όσο και τομεακή, μεταξύ άλλων όσον αφορά τη δημόσια ασφάλεια, την άμυνα, την εθνική ασφάλεια και το ποινικό δίκαιο και την πρόσβαση των δημόσιων αρχών στα δεδομένα προσωπικού χαρακτήρα, καθώς και την εφαρμογή της νομοθεσίας αυτής, τους κανόνες περί προστασίας δεδομένων, τους επαγγελματικούς κανόνες και τα μέτρα ασφαλείας, συμπεριλαμβανομένων των κανόνων περί περαιτέρω διαβιβάσεων δεδομένων προσωπικού χαρακτήρα σε άλλη τρίτη χώρα ή διεθνή οργανισμό, που τηρούνται στην εν λόγω χώρα ή διεθνή οργανισμό, τη νομολογία και επίσης τα αποτελεσματικά και εκτελεστά δικαιώματα των υποκειμένων των δεδομένων και τα αποτελεσματικά διοικητικά και δικαστικά μέσα προσφυγής για τα υποκείμενα των δεδομένων των οποίων διαβιβάζονται δεδομένα προσωπικού χαρακτήρα, β) την ύπαρξη και την αποτελεσματική λειτουργία μίας ή περισσότερων ανεξάρτητων εποπτικών αρχών στην τρίτη χώρα ή στην οποία ή στις οποίες υπόκειται ένας διεθνής οργανισμός, με ευθύνη τη διασφάλιση και την επιβολή της συμμόρφωσης προς τους κανόνες προστασίας των δεδομένων, περιλαμβανομένων κατάλληλων εξουσιών για την επιβολή κυρώσεων, για την παροχή συνδρομής και ενημέρωσης στα υποκείμενα των δεδομένων κατά την άσκηση των δικαιωμάτων τους και για τη συνεργασία με τον επίτροπο και γ) τις διεθνείς δεσμεύσεις που έχει αναλάβει η οικεία τρίτη χώρα ή διεθνής οργανισμός ή άλλες υποχρεώσεις οι οποίες απορρέουν από νομικά δεσμευτικές συμβάσεις ή πράξεις καθώς και από τη συμμετοχή τους σε πολυμερή ή περιφερειακά συστήματα, ιδίως όσον αφορά την προστασία δεδομένων προσωπικού χαρακτήρα».

Επίτροπο Πληροφοριών όταν προτείνει τη θέσπιση μελλοντικών κανονισμών του Ηνωμένου Βασιλείου περί επάρκειας ([143]). Μόλις εγκριθούν από τον ανώτερο υπουργό, οι εν λόγω κανονισμοί υποβάλλονται στο Κοινοβούλιο και υπόκεινται στη διαδικασία «αρνητικής απόφασης», σύμφωνα με την οποία αμφότερα τα σώματα του Κοινοβουλίου μπορούν να εξετάσουν ενδελεχώς τον κανονισμό και έχουν τη δυνατότητα να εγκρίνουν πρόταση ακύρωσής του εντός προθεσμίας 40 ημερών ([144]).

(78) Σύμφωνα με το άρθρο 74Β παράγραφος 1 του DPA 2018, οι κανονισμοί περί επάρκειας πρέπει να επανεξετάζονται ανά διαστήματα τα οποία να μην υπερβαίνουν τα τέσσερα έτη και ο ανώτερος υπουργός πρέπει, σε συνεχή βάση, να παρακολουθεί τις εξελίξεις σε τρίτες χώρες και διεθνείς οργανισμούς οι οποίες θα μπορούσαν να επηρεάσουν τις αποφάσεις για τη θέσπιση κανονισμών περί επάρκειας ή για την τροποποίηση ή την ανάκληση των εν λόγω κανονισμών. Όταν ανώτερος ο υπουργός διαπιστώνει ότι μια συγκεκριμένη χώρα ή ένας οργανισμός δεν εξασφαλίζει πλέον επαρκές επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα, πρέπει, στον βαθμό που είναι αναγκαίο, να τροποποιεί ή να ανακαλεί τους κανονισμούς και να αρχίζει διαβουλεύσεις με την οικεία τρίτη χώρα ή τον οικείο διεθνή οργανισμό για να διορθώσει την έλλειψη επαρκούς επιπέδου προστασίας.

(79) Όπως προβλέπεται και στο άρθρο 37 της οδηγίας (ΕΕ) 2016/680, ελλείψει κανονισμού περί επάρκειας, η διαβίβαση δεδομένων προσωπικού χαρακτήρα στο πλαίσιο του τομέα της επιβολής του νόμου θα ήταν δυνατή όταν υφίστανται κατάλληλες εγγυήσεις. Οι εν λόγω εγγυήσεις διασφαλίζονται είτε μέσω α) νομικά δεσμευτικής πράξης που περιέχει κατάλληλες εγγυήσεις για την προστασία των δεδομένων προσωπικού χαρακτήρα· είτε μέσω β) εκτίμησης που διενεργείται από τον υπεύθυνο επεξεργασίας ο οποίος, αφού αξιολογήσει όλες τις περιστάσεις που περιβάλλουν τη διαβίβαση, καταλήγει στο συμπέρασμα ότι υφίστανται οι κατάλληλες εγγυήσεις για την προστασία των δεδομένων ([145]). Επιπλέον, όταν οι διαβιβάσεις βασίζονται σε κατάλληλες εγγυήσεις, ο DPA 2018 προβλέπει ότι, πέραν του συνήθους εποπτικού ρόλου του ICO, οι αρμόδιες αρχές πρέπει να παρέχουν συγκεκριμένες πληροφορίες σχετικά με τις διαβιβάσεις στο ICO ([146]).

(80) Εάν η διαβίβαση δεν βασίζεται σε απόφαση περί επάρκειας ή σε κατάλληλες εγγυήσεις, μπορεί να πραγματοποιηθεί μόνο σε ορισμένες, συγκεκριμένες περιστάσεις, οι οποίες αναφέρονται ως «ειδικές περιστάσεις» ([147]). Αυτό συμβαίνει όταν η διαβίβαση είναι αναγκαία: α) για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου προσώπου· β) για την προστασία έννομων συμφερόντων του υποκειμένου των δεδομένων· γ) για την αποτροπή άμεσης και σοβαρής απειλής για τη δημόσια ασφάλεια κράτους μέλους ή τρίτης χώρας· δ) σε μεμονωμένες περιπτώσεις για τους σκοπούς επιβολής του νόμου· ή ε) σε μεμονωμένες περιπτώσεις για νόμιμο σκοπό (όπως στο πλαίσιο νομικών διαδικασιών ή για τη λήψη νομικών συμβουλών) ([148]). Επισημαίνεται ότι τα στοιχεία δ) και ε) δεν εφαρμόζονται εάν τα δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων υπερισχύουν του δημόσιου συμφέροντος της διαβίβασης ([149]). Αυτό το σύνολο περιστάσεων αντιστοιχεί στις ειδικές καταστάσεις και προϋποθέσεις που χαρακτηρίζονται ως «παρεκκλίσεις» βάσει του άρθρου 38 της οδηγίας (ΕΕ) 2016/680.

(81) Υπό τις περιστάσεις αυτές, η ημερομηνία, η ώρα και η αιτιολόγηση της διαβίβασης, το όνομα και κάθε άλλη σχετική πληροφορία για τον αποδέκτη, καθώς και η περιγραφή των διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα πρέπει να τεκμηριώνονται και να παρέχονται στον Επίτροπο Πληροφοριών κατόπιν αιτήματος ([150]).

(82) Το άρθρο 78 του DPA 2018 ρυθμίζει την περίπτωση των «μεταγενέστερων διαβιβάσεων», συγκεκριμένα όταν δεδομένα προσωπικού χαρακτήρα που έχουν διαβιβαστεί από το Ηνωμένο Βασίλειο σε τρίτη χώρα διαβιβάζονται στη συνέχεια σε άλλη τρίτη χώρα ή σε διεθνή οργανισμό. Σύμφωνα με το άρθρο 78 παράγραφος 1, ο διαβιβάζων υπεύθυνος επεξεργασίας του Ηνωμένου Βασιλείου πρέπει να θέσει ως προϋπόθεση της διαβίβασης ότι τα δεδομένα δεν πρέπει να διαβιβαστούν περαιτέρω σε τρίτη χώρα χωρίς την έγκριση του διαβιβάζοντος υπευθύνου επεξεργασίας. Επιπλέον, σύμφωνα με το άρθρο 78 παράγραφος 3 και όπως προβλέπεται στο άρθρο 35 παράγραφος 1 στοιχείο ε) της οδηγίας (ΕΕ) 2016/680, σε περίπτωση που απαιτείται τέτοια άδεια, ισχύουν ορισμένες ουσιαστικές απαιτήσεις. Ειδικότερα, όταν αποφασίζει αν θα εγκρίνει ή όχι τη διαβίβαση, η αρμόδια αρχή πρέπει να διασφαλίζει ότι η περαιτέρω διαβίβαση είναι αναγκαία για σκοπούς

([143]) Βλέπε το μνημόνιο συμφωνίας μεταξύ του υπουργού Ψηφιακής Πολιτικής, Πολιτισμού, Μέσων Μαζικής Ενημέρωσης και Αθλητισμού (Department for Digital, Culture, Media and Sport, DCMS) και του Γραφείου του Επιτρόπου Πληροφοριών σχετικά με τον ρόλο του ICO όσον αφορά τη νέα αξιολόγηση επάρκειας του Ηνωμένου Βασιλείου, το οποίο είναι διαθέσιμο στον σύνδεσμο https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([144]) Κατά τη διάρκεια αυτής της περιόδου 40 ημερών, αμφότερα τα σώματα του Κοινοβουλίου μπορούν να έχουν την ευκαιρία, εφόσον το επιθυμούν, να καταψηφίσουν τους κανονισμούς· σε περίπτωση καταψήφισής τους, οι κανονισμοί θα παύσουν τελικά να παράγουν περαιτέρω έννομα αποτελέσματα.

([145]) Άρθρο 75 του DPA 2018.

([146]) Σύμφωνα με το άρθρο 75 παράγραφος 3 του DPA 2018, όταν πραγματοποιείται διαβίβαση δεδομένων βάσει κατάλληλων εγγυήσεων: α) η διαβίβαση πρέπει να τεκμηριώνεται, β) η τεκμηρίωση πρέπει να υποβάλλεται στον επίτροπο κατόπιν αιτήματος και γ) η τεκμηρίωση πρέπει να περιλαμβάνει, ειδικότερα i) την ημερομηνία και την ώρα της διαβίβασης, ii) το όνομα και κάθε άλλη συναφή πληροφορία σχετικά με τον αποδέκτη, iii) την αιτιολόγηση της διαβίβασης και iv) περιγραφή των διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα.

([147]) Guide to Law Enforcement Processing, «Are there any special circumstances?», διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3.

([148]) Άρθρο 76 του DPA 2018.

([149]) Άρθρο 76 του DPA 2018.

([150]) Άρθρο 76 παράγραφος 3 του DPA 2018.

επιβολής του νόμου και θα πρέπει να εξετάζει, μεταξύ άλλων παραγόντων, α) τη σοβαρότητα των περιστάσεων που οδήγησαν στην αίτηση έγκρισης, β) τον σκοπό για τον οποίο διαβιβάστηκαν αρχικά τα δεδομένα προσωπικού χαρακτήρα και γ) τα πρότυπα για την προστασία των δεδομένων προσωπικού χαρακτήρα που ισχύουν στην τρίτη χώρα ή στον διεθνή οργανισμό στην οποία/στον οποίο θα διαβιβαστούν τα δεδομένα προσωπικού χαρακτήρα.

(83) Επιπλέον, όταν τα δεδομένα που υπόκεινται σε περαιτέρω διαβίβαση από το Ηνωμένο Βασίλειο διαβιβάστηκαν αρχικά από την Ευρωπαϊκή Ένωση, ισχύουν πρόσθετες εγγυήσεις.

(84) Πρώτον, το άρθρο 73 παράγραφος 1 στοιχείο b) του DPA 2018 –όπως και το άρθρο 35 παράγραφος 1 στοιχείο γ) της οδηγίας (ΕΕ) 2016/680– προβλέπει ότι σε περίπτωση που τα δεδομένα προσωπικού χαρακτήρα αρχικά διαβιβάστηκαν ή διατέθηκαν με άλλον τρόπο στον υπεύθυνο επεξεργασίας ή σε άλλη αρμόδια αρχή από κράτος μέλος, το εν λόγω κράτος μέλος, ή οποιοδήποτε πρόσωπο εγκατεστημένο στο εν λόγω κράτος μέλος το οποίο είναι αρμόδια αρχή για τους σκοπούς της οδηγίας (ΕΕ) 2016/680, πρέπει να έχει επιτρέψει τη διαβίβαση σύμφωνα με το δίκαιο του κράτους μέλους.

(85) Ωστόσο, όπως και στο άρθρο 35 παράγραφος 2, της οδηγίας (ΕΕ) 2016/680, η σχετική έγκριση δεν απαιτείται όταν α) η διαβίβαση είναι αναγκαία για την αποτροπή άμεσης και σοβαρής απειλής είτε για τη δημόσια ασφάλεια κράτους μέλους ή τρίτης χώρας είτε για τα ουσιώδη συμφέροντα κράτους μέλους και β) η έγκριση δεν μπορεί να ληφθεί εγκαίρως. Στην περίπτωση αυτή, η αρχή του κράτους μέλους που θα ήταν υπεύθυνη να αποφασίσει αν θα εγκρίνει τη διαβίβαση πρέπει να ενημερώνεται χωρίς καθυστέρηση ([151]).

(86) Δεύτερον, η ίδια προσέγγιση ισχύει και στην περίπτωση δεδομένων που αρχικά διαβιβάστηκαν από την Ευρωπαϊκή Ένωση στο Ηνωμένο Βασίλειο και στη συνέχεια διαβιβάζονται περαιτέρω από το Ηνωμένο Βασίλειο σε τρίτη χώρα η οποία στη συνέχεια τα διαβιβάζει περαιτέρω σε τρίτη χώρα. Στην περίπτωση αυτή, σύμφωνα με το άρθρο 78 παράγραφος 4, η αρμόδια αρχή του Ηνωμένου Βασιλείου δεν μπορεί να χορηγήσει την άδειά της στην τελευταία διαβίβαση, σύμφωνα με το άρθρο 78 παράγραφος 1, εκτός εάν το «κράτος μέλος [το οποίο διαβίβασε αρχικά τα εν λόγω δεδομένα], ή οποιοδήποτε πρόσωπο με έδρα στο εν λόγω κράτος μέλος το οποίο είναι αρμόδια αρχή για τους σκοπούς της οδηγίας για την προστασία των δεδομένων στο πλαίσιο της επιβολής του νόμου, έχει επιτρέψει τη διαβίβαση σύμφωνα με το δίκαιο του κράτους μέλους». Οι εγγυήσεις αυτές είναι σημαντικές, καθώς επιτρέπουν στις αρχές των κρατών μελών να διασφαλίζουν τη συνέχεια της προστασίας, σε συμμόρφωση με την ενωσιακή νομοθεσία για την προστασία των δεδομένων, σε όλο το μήκος της «αλυσίδας διαβίβασης».

(87) Το νέο αυτό πλαίσιο για τις διεθνείς διαβιβάσεις τέθηκε σε εφαρμογή κατά τη λήξη της μεταβατικής περιόδου ([152]). Ωστόσο, σύμφωνα με τις παραγράφους 10-12 του παραρτήματος 21 (που θεσπίστηκαν με τους κανονισμούς DPPEC) προβλέπεται ότι, από τη λήξη της μεταβατικής περιόδου, ορισμένες διαβιβάσεις δεδομένων προσωπικού χαρακτήρα αντιμετωπίζονται ωσάν να βασίζονται σε κανονισμούς περί επάρκειας. Οι εν λόγω διαβιβάσεις περιλαμβάνουν διαβιβάσεις σε κράτος μέλος, σε κράτος της ΕΖΕΣ, τρίτη χώρα που αποτελεί αντικείμενο ενωσιακής απόφασης επάρκειας κατά τη λήξη της μεταβατικής περιόδου και το έδαφος του Γιβραλτάρ. Κατά συνέπεια, οι διαβιβάσεις προς τις χώρες αυτές μπορούν να συνεχιστούν όπως και πριν από την αποχώρηση του Ηνωμένου Βασιλείου από την Ένωση. Μετά τη λήξη της μεταβατικής περιόδου, ο ανώτερος υπουργός πρέπει να προβεί σε επανεξέταση των διαπιστώσεων επάρκειας εντός περιόδου τεσσάρων ετών, δηλαδή έως το τέλος Δεκεμβρίου του 2024. Σύμφωνα με την εξήγηση που έδωσαν οι αρχές του Ηνωμένου Βασιλείου, μολονότι ο ανώτερος υπουργός πρέπει να προβεί στην εν λόγω επανεξέταση έως το τέλος Δεκεμβρίου του 2024, οι μεταβατικές διατάξεις δεν περιλαμβάνουν διάταξη «λήξης ισχύος» και οι σχετικές μεταβατικές διατάξεις δεν θα παύσουν αυτομάτως να παράγουν αποτελέσματα εάν η επανεξέταση δεν ολοκληρωθεί έως το τέλος Δεκεμβρίου του 2024.

2.4.9. *Λογοδοσία*

(88) Βάσει της αρχής της λογοδοσίας, οι δημόσιες αρχές που υποβάλλουν σε επεξεργασία δεδομένα πρέπει να θεσπίζουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα προκειμένου να συμμορφώνονται ουσιαστικά με τις υποχρεώσεις τους όσον αφορά την προστασία των δεδομένων και να είναι σε θέση να αποδεικνύουν τη συμμόρφωσή τους, ειδικά στην αρμόδια εποπτική αρχή.

(89) Η αρχή αυτή αντικατοπτρίζεται στο άρθρο 56 του DPA 2018, ο οποίος θεσπίζει γενική υποχρέωση λογοδοσίας για τον υπεύθυνο επεξεργασίας, δηλαδή την υποχρέωσή του να εφαρμόζει κατάλληλα τεχνικά και οργανωτικά μέτρα ώστε να διασφαλίζει, και να είναι σε θέση να αποδεικνύει, ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα συμμορφώνεται με τις απαιτήσεις του μέρους 3 του DPA 2018. Τα μέτρα που εφαρμόζονται πρέπει να επανεξετάζονται και να επικαιροποιούνται όπου είναι αναγκαίο και, όταν δικαιολογούνται σε σχέση με την επεξεργασία, πρέπει να περιλαμβάνουν κατάλληλες πολιτικές για την προστασία των δεδομένων.

([151]) Άρθρο 73 παράγραφος 5 του DPA 2018.

([152]) Η δυνατότητα εφαρμογής αυτού του νέου πλαισίου πρέπει να εξεταστεί υπό το πρίσμα του άρθρου 782 της συμφωνίας εμπορίου και συνεργασίας μεταξύ της Ευρωπαϊκής Ένωσης και της Ευρωπαϊκής Κοινότητας Ατομικής Ενέργειας, αφενός, και του Ηνωμένου Βασιλείου της Μεγάλης Βρετανίας και της Βόρειας Ιρλανδίας, αφετέρου (L 444/14 της 31.12.2020) (στο εξής: ΣΕΣ ΕΕ–Ηνωμένου Βασιλείου), που διατίθεται στον ακόλουθο σύνδεσμο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EL.

(90) Σύμφωνα με το κεφάλαιο IV της οδηγίας (ΕΕ) 2016/680, τα άρθρα 55-71 του DPA 2018 προβλέπουν διαφορετικούς μηχανισμούς για τη διασφάλιση της λογοδοσίας και την παροχή δυνατότητας στους υπευθύνους επεξεργασίας και στους εκτελούντες την επεξεργασία να αποδεικνύουν τη συμμόρφωση. Ειδικότερα, οι υπεύθυνοι επεξεργασίας υποχρεούνται να εφαρμόζουν μέτρα προστασίας των δεδομένων από τον σχεδιασμό και εξ ορισμού, δηλαδή να διασφαλίζουν ότι οι αρχές προστασίας των δεδομένων εφαρμόζονται αποτελεσματικά, και υποχρεούνται να τηρούν αρχεία όλων των κατηγοριών δραστηριοτήτων επεξεργασίας για τις οποίες φέρει την ευθύνη ο υπεύθυνος επεξεργασίας (συμπεριλαμβανομένων των πληροφοριών σχετικά με την ταυτότητα του υπευθύνου επεξεργασίας, τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων, τους σκοπούς της επεξεργασίας, τις κατηγορίες αποδεκτών των κοινολογήσεων και περιγραφή των κατηγοριών των υποκειμένων των δεδομένων και των δεδομένων προσωπικού χαρακτήρα) και να τηρούν τα αρχεία αυτά στη διάθεση του Επιτρόπου Πληροφοριών κατόπιν αιτήματος. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία πρέπει επίσης να τηρούν αρχεία καταχώρισης για ορισμένες πράξεις επεξεργασίας και να τα θέτουν στη διάθεση του Επιτρόπου Πληροφοριών ([153]). Οι υπεύθυνοι επεξεργασίας υποχρεούνται επίσης ρητά να συνεργάζονται με τον Επίτροπο Πληροφοριών κατά την εκτέλεση των καθηκόντων του.

(91) Ο DPA 2018 προβλέπει επίσης πρόσθετες απαιτήσεις για την επεξεργασία που ενδέχεται να έχει ως αποτέλεσμα μεγάλο κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Σ' αυτές περιλαμβάνεται η υποχρέωση διενέργειας εκτιμήσεων επιπτώσεων σχετικά με την προστασία των δεδομένων και διαβούλευσης με τον Επίτροπο Πληροφοριών πριν από την επεξεργασία, εάν η εν λόγω εκτίμηση υποδεικνύει ότι η επεξεργασία θα είχε ως αποτέλεσμα υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες φυσικών προσώπων (ελλείψει μέτρων για τον μετριασμό του κινδύνου).

(92) Επιπλέον, οι υπεύθυνοι επεξεργασίας πρέπει να διορίζουν υπεύθυνο προστασίας δεδομένων, εκτός εάν ο υπεύθυνος επεξεργασίας είναι δικαστήριο ή άλλη δικαστική αρχή που ενεργεί στο πλαίσιο της δικαιοδοτικής του/της αρμοδιότητας ([154]). Ο υπεύθυνος επεξεργασίας πρέπει να διασφαλίζει ότι ο υπεύθυνος προστασίας δεδομένων συμμετέχει σε όλα τα ζητήματα που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα, να διαθέτει τους απαραίτητους πόρους και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, και να μπορεί να εκτελεί ανεξάρτητα τα καθήκοντά του. Τα καθήκοντα του υπευθύνου προστασίας δεδομένων ορίζονται στο άρθρο 71 του DPA 2018, συμπεριλαμβανομένης της παροχής πληροφοριών και συμβουλών, της παρακολούθησης της συμμόρφωσης, καθώς και της συνεργασίας με τον Επίτροπο Πληροφοριών και του ρόλου του ως σημείου επαφής μαζί του. Κατά την εκτέλεση των καθηκόντων του, ο υπεύθυνος προστασίας δεδομένων πρέπει να λαμβάνει υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.

2.5. **Εποπτεία και επιβολή**

2.5.1. *Ανεξάρτητη εποπτεία*

(93) Για να είναι εγγυημένη η διασφάλιση επαρκούς επιπέδου προστασίας των δεδομένων και στην πράξη, είναι αναγκαία η ίδρυση ανεξάρτητης εποπτικής αρχής στην οποία ανατίθενται εξουσίες παρακολούθησης και επιβολής της συμμόρφωσης με τους κανόνες προστασίας των δεδομένων. Η αρχή αυτή πρέπει να λειτουργεί με πλήρη ανεξαρτησία και αμεροληψία κατά την εκτέλεση των καθηκόντων και την άσκηση των εξουσιών της.

(94) Στο Ηνωμένο Βασίλειο, ο Επίτροπος Πληροφοριών διενεργεί την εποπτεία και την επιβολή της συμμόρφωσης με τον ΓΚΠΔ του Ηνωμένου Βασιλείου και τον DPA 2018 ([155]). Ο Επίτροπος Πληροφοριών εποπτεύει επίσης την επεξεργασία δεδομένων προσωπικού χαρακτήρα από αρμόδιες αρχές η οποία εμπίπτει στο πεδίο εφαρμογής του μέρους 3 του DPA 2018 ([156]). Ο Επίτροπος Πληροφοριών είναι ειδικής μορφής νομικό πρόσωπο (Corporation Sole): χωριστή νομική οντότητα που συνίσταται σε ένα και μόνο πρόσωπο. Ο Επίτροπος Πληροφοριών υποστηρίζεται στο έργο του από γραφείο. Στις 31 Μαρτίου 2020 το Γραφείο του Επιτρόπου Πληροφοριών είχε 768 μόνιμους υπαλλήλους ως προσωπικό ([157]). Το υπουργείο που χρηματοδοτεί τον Επίτροπο Πληροφοριών είναι το υπουργείο Ψηφιακής Πολιτικής, Πολιτισμού, Μέσων Μαζικής Ενημέρωσης και Αθλητισμού ([158]).

([153]) Άρθρο 62 του DPA 2018.

([154]) Άρθρο 69 του DPA 2018.

([155]) Άρθρο 36 παράγραφος 2 στοιχείο β) της οδηγίας (ΕΕ) 2016/680.

([156]) Άρθρο 116 του DPA 2018.

([157]) Information Commissioner's Annual Report and Financial Statements 2019-2020, διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf.

([158]) Η σχέση μεταξύ Επιτρόπου και υπουργείου ρυθμίζεται από συμφωνία διαχείρισης (Management Agreement). Ειδικότερα, οι βασικές αρμοδιότητες του υπουργείου Ψηφιακής Πολιτικής, Πολιτισμού, Μέσων Μαζικής Ενημέρωσης και Αθλητισμού, ως χρηματοδοτούντος υπουργείου, περιλαμβάνουν τα εξής: τη διασφάλιση της παροχής επαρκούς χρηματοδότησης και πόρων στο ICO· την εκπροσώπηση των συμφερόντων του ICO στο Κοινοβούλιο και σε άλλες κυβερνητικές υπηρεσίες· τη διασφάλιση της ύπαρξης ισχυρού εθνικού πλαισίου προστασίας των δεδομένων· και την παροχή καθοδήγησης και στήριξης στο ICO σχετικά με εταιρικά ζητήματα, όπως ζητήματα ακινήτων, μισθώσεων και δημόσιων συμβάσεων (η συμφωνία διαχείρισης 2018-2021 διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) Η ανεξαρτησία του Επιτρόπου κατοχυρώνεται ρητά στο άρθρο 52 του ΓΚΠΔ του Ηνωμένου Βασιλείου, το οποίο αντικατοπτρίζει τις απαιτήσεις που ορίζονται στο άρθρο 52 παράγραφοι 1 έως 3 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([159]). Ο Επίτροπος πρέπει να εκτελεί τα καθήκοντά του και να ασκεί τις εξουσίες του με πλήρη ανεξαρτησία σύμφωνα με τον ΓΚΠΔ του Ηνωμένου Βασιλείου, χωρίς εξωτερικές επιρροές, είτε άμεσες είτε έμμεσες, σε σχέση με τα εν λόγω καθήκοντα και εξουσίες, και να μην ζητεί ούτε να λαμβάνει οδηγίες από κανέναν. Ο Επίτροπος πρέπει επίσης να απέχει από κάθε πράξη ασυμβίβαστη προς τα καθήκοντά του και, κατά τη διάρκεια της θητείας του, να μην ασκεί κανένα ασυμβίβαστο επάγγελμα, επικερδές ή μη.

(96) Οι προϋποθέσεις για τον διορισμό και την παύση του Επιτρόπου Πληροφοριών καθορίζονται στο παράρτημα 12 του DPA 2018. Ο Επίτροπος Πληροφοριών διορίζεται από τη Βασίλισσα μετά από σύσταση της κυβέρνησης βάσει δίκαιου και ανοικτού διαγωνισμού. Ο υποψήφιος πρέπει να διαθέτει τα κατάλληλα προσόντα, δεξιότητες και ικανότητες. Σύμφωνα με τον κώδικα διακυβέρνησης για τους δημόσιους διορισμούς ([160]), συμβουλευτική επιτροπή αξιολόγησης καταρτίζει κατάλογο με τους υποψήφιους που μπορούν να διοριστούν. Πριν από την οριστικοποίηση της απόφασης του ανώτερου υπουργού Ψηφιακής Πολιτικής, Πολιτισμού, Μέσων Ενημέρωσης και Αθλητισμού, η αρμόδια ειδική επιτροπή (Select Committee) του Κοινοβουλίου πρέπει να διενεργεί έλεγχο πριν από τον διορισμό. Η θέση της επιτροπής δημοσιοποιείται ([161]).

(97) Ο Επίτροπος Πληροφοριών ασκεί θητεία έως επτά ετών. Ο Επίτροπος Πληροφοριών μπορεί να παυθεί από τα καθήκοντά του από την Αυτής Μεγαλειότητα μετά από αναγγελία και των δύο σωμάτων του Κοινοβουλίου ([162]). Δεν μπορεί να υποβληθεί αίτηση παύσης του επιτρόπου Πληροφοριών σε κανένα από τα δύο σώματα του Κοινοβουλίου, εκτός εάν ο υπουργός έχει υποβάλει έκθεση στο σχετικό σώμα στην οποία αναφέρεται ότι είναι πεπεισμένος ότι ο επίτροπος Πληροφοριών είναι ένοχος σοβαρού παραπτώματος και/ή ότι ο επίτροπος δεν πληροί πλέον τις προϋποθέσεις που απαιτούνται για την άσκηση των καθηκόντων του ([163]).

(98) Η χρηματοδότηση του επιτρόπου Πληροφοριών προέρχεται από τρεις πηγές: i) τα τέλη προστασίας δεδομένων που καταβάλλουν οι υπεύθυνοι επεξεργασίας, τα οποία καθορίζονται από κανονισμούς του υπουργού ([164]) και ανέρχονται στο 85-90 % του ετήσιου προϋπολογισμού του Γραφείου ([165])· ii) την επιχορήγηση που μπορεί να καταβάλει η κυβέρνηση στον επίτροπο Πληροφοριών και η οποία χρησιμοποιείται κυρίως για τη χρηματοδότηση των λειτουργικών δαπανών του επιτρόπου Πληροφοριών όσον αφορά καθήκοντα που δεν σχετίζονται με την προστασία των δεδομένων ([166])· iii) τα τέλη που χρεώνονται για υπηρεσίες ([167]). Επί του παρόντος, δεν χρεώνονται τα εν λόγω τέλη.

(99) Τα γενικά καθήκοντα του Επιτρόπου Πληροφοριών σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που εμπίπτει στο πεδίο εφαρμογής του μέρους 3 του DPA 2018 καθορίζονται στο παράρτημα 13 του εν λόγω νόμου. Στα καθήκοντα περιλαμβάνονται η παρακολούθηση και η επιβολή του μέρους 3 του DPA 2018, η προώθηση της ευαισθητοποίησης του κοινού, η παροχή συμβουλών στο Κοινοβούλιο, στην κυβέρνηση και σε άλλα όργανα όσον αφορά νομοθετικά και διοικητικά μέτρα, η προώθηση της ευαισθητοποίησης των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία σχετικά με τις υποχρεώσεις τους, η παροχή πληροφοριών στο υποκείμενο των δεδομένων σχετικά με την

([159]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

([160]) Governance Code on Public Appointments, διατίθεται στον ακόλουθο σύνδεσμο: https://www.gov.uk/government/publications/governance-code-for-public-appointments.

([161]) Second Report of Session 2015-2016 of the Culture, Media and Sports Committee at the House of Commons, διατίθεται στον ακόλουθο σύνδεσμο: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf.

([162]) Η «αναγγελία» (address) είναι αίτηση που κατατίθεται στο Κοινοβούλιο με την οποία ζητείται να ενημερωθεί ο μονάρχης σχετικά με τη γνώμη του Κοινοβουλίου για συγκεκριμένο ζήτημα.

([163]) Παράρτημα 12 παράγραφος 3 του DPA 2018.

([164]) Άρθρο 137 του DPA 2018.

([165]) Τα άρθρα 137 και 138 του DPA 2018 περιέχουν ορισμένες εγγυήσεις για τη διασφάλιση του καθορισμού των τελών σε κατάλληλο επίπεδο. Ειδικότερα, το άρθρο 137 παράγραφος 4 του DPA 2018 απαριθμεί τα θέματα που πρέπει να λαμβάνει υπόψη του ο ανώτερος υπουργός κατά τη θέσπιση κανονισμών που καθορίζουν το ποσό που πρέπει να καταβάλλουν οι διάφοροι οργανισμοί. Το άρθρο 138 παράγραφος 1 και το άρθρο 182 του DPA 2018 περιλαμβάνει επίσης τη νομική υποχρέωση του ανώτερου υπουργού να διαβουλεύεται με τον Επίτροπο Πληροφοριών και άλλους εκπροσώπους των προσώπων που ενδέχεται να θιγούν από τους κανονισμούς, πριν από τη θέσπισή τους προκειμένου να ληφθούν υπόψη οι απόψεις τους. Επιπλέον, σύμφωνα με το άρθρο 138 παράγραφος 2 του DPA 2018, ο Επίτροπος Πληροφοριών υποχρεούται να επανεξετάζει τη λειτουργία των κανονισμών περί τελών και μπορεί να υποβάλλει προτάσεις στον ανώτερο υπουργό για τροποποιήσεις των κανονισμών. Τέλος, εκτός από τις περιπτώσεις στις οποίες οι κανονισμοί εκδίδονται απλώς για να ληφθεί υπόψη η αύξηση του δείκτη τιμών λιανικής (οπότε θα υπόκεινται στη διαδικασία αρνητικού ψηφίσματος), οι κανονισμοί υπόκεινται στη διαδικασία θετικού ψηφίσματος και μπορούν να θεσπιστούν μόνο μετά την έγκρισή τους με ψήφισμα από κάθε σώμα του Κοινοβουλίου.

([166]) Στη συμφωνία διαχείρισης διευκρινίζεται ότι «Ο ανώτερος υπουργός μπορεί να προβαίνει σε πληρωμές προς τον Επίτροπο Πληροφοριών από κονδύλια χορηγούμενα από το Κοινοβούλιο σύμφωνα με το παράρτημα 12 παράγραφος 9 του DPA 2018. Αφού ζητήσει τη γνώμη του Επιτρόπου Πληροφοριών, το υπουργείο Ψηφιακής Πολιτικής, Πολιτισμού, Μέσων Μαζικής Ενημέρωσης και Αθλητισμού καταβάλλει στον Επίτροπο Πληροφοριών τα κατάλληλα ποσά (επιχορήγηση) για τις διοικητικές δαπάνες του ICO και την άσκηση των καθηκόντων του Επιτρόπου Πληροφοριών σε σχέση με ορισμένα ειδικά καθήκοντα, συμπεριλαμβανομένης της ελευθερίας της πληροφόρησης» (Management Agreement 2018-2021, παράγραφος 1.12, βλέπε υποσημείωση 158).

([167]) Άρθρο 134 του DPA 2018.

άσκηση των δικαιωμάτων του και η διεξαγωγή ερευνών. Για τη διατήρηση της ανεξαρτησίας της δικαστικής εξουσίας, ο Επίτροπος Πληροφοριών δεν έχει την εξουσία να ασκεί τα καθήκοντά του σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από πρόσωπο ή δικαστήριο ή δικαιοδοτικό όργανο που ενεργεί στο πλαίσιο της δικαιοδοτικής του αρμοδιότητας. Ωστόσο, η εποπτεία της δικαστικής εξουσίας εξασφαλίζεται από εξειδικευμένα όργανα, τα οποία εξετάζονται κατωτέρω.

2.5.1.1 Επιβολή, συμπεριλαμβανομένων των κυρώσεων

(100) Ο Επίτροπος διαθέτει γενικές ερευνητικές, διορθωτικές, αδειοδοτικές και συμβουλευτικές εξουσίες σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα η οποία διέπεται από το μέρος 3 του DPA 2018. Ο Επίτροπος έχει την εξουσία να ενημερώνει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία για εικαζόμενη παράβαση του μέρους 3, να απευθύνει προειδοποιήσεις σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία ότι σκοπούμενες πράξεις επεξεργασίας είναι πιθανόν να παραβαίνουν τις διατάξεις του μέρους 3 και να απευθύνει επιπλήξεις σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία όταν πράξεις επεξεργασίας έχουν παραβεί διατάξεις του μέρους 3. Επιπροσθέτως, ο Επίτροπος, με δική του πρωτοβουλία ή κατόπιν αιτήματος, δύναται να εκδίδει γνωμοδοτήσεις προς το Κοινοβούλιο, την κυβέρνηση ή άλλα όργανα και οργανισμούς του Ηνωμένου Βασιλείου, καθώς και προς το κοινό, για κάθε θέμα το οποίο σχετίζεται με την προστασία των δεδομένων προσωπικού χαρακτήρα ([168]).

(101) Επιπλέον, ο Επίτροπος έχει την εξουσία:

— να διατάσσει τον υπεύθυνο επεξεργασίας και τον εκτελούντα την επεξεργασία (και, σε ορισμένες περιπτώσεις, οποιοδήποτε άλλο πρόσωπο) να παράσχουν τις αναγκαίες πληροφορίες μέσω ειδοποίησης παροχής πληροφοριών (στο εξής: ειδοποίηση παροχής πληροφοριών) ([169])·

— να διεξάγει έρευνες και ελέγχους μέσω ειδοποίησης διενέργειας αξιολόγησης, στο πλαίσιο των οποίων ενδέχεται να υποχρεωθεί ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία να επιτρέψει στον Επίτροπο να εισέλθει σε συγκεκριμένες εγκαταστάσεις, να επιθεωρήσει ή να εξετάσει έγγραφα ή εξοπλισμό και να υποβάλει ερωτήσεις σε πρόσωπα που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας (στο εξής: ειδοποίηση διενέργειας αξιολόγησης) ([170])·

— να αποκτά με άλλον τρόπο πρόσβαση στα έγγραφα των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία, καθώς και πρόσβαση στις εγκαταστάσεις τους σύμφωνα με το άρθρο 154 του DPA 2018 (στο εξής: εξουσίες εισόδου και διενέργειας επιθεώρησης)·

— να ασκεί διορθωτικές εξουσίες, μεταξύ άλλων, μέσω προειδοποιήσεων και επιπλήξεων, ή να δίνει εντολές μέσω ειδοποιήσεων επιβολής μέτρων που να απαιτούν από τους υπευθύνους επεξεργασίας/εκτελούντες την επεξεργασία να λαμβάνουν συγκεκριμένα μέτρα ή να απέχουν από τη λήψη μέτρων (στο εξής: ειδοποίηση επιβολής μέτρων) ([171])· και

— να επιβάλλει διοικητικά πρόστιμα με τη μορφή ειδοποίησης επιβολής κυρώσεων (στο εξής: ειδοποίηση επιβολής κυρώσεων) ([172]).

(102) Η πολιτική ρυθμιστικής δράσης του ICO καθορίζει τις περιστάσεις υπό τις οποίες ο Επίτροπος θα εκδίδει, αντίστοιχα, ειδοποίηση παροχής πληροφοριών, διενέργειας αξιολόγησης, επιβολής μέτρων και επιβολής κυρώσεων ([173]). Η ειδοποίηση επιβολής μέτρων μπορεί να επιβάλλει απαιτήσεις τις οποίες ο Επίτροπος θεωρεί κατάλληλες για τους σκοπούς της επανόρθωσης της μη συμμόρφωσης. Η ειδοποίηση επιβολής κυρώσεων απαιτεί από το πρόσωπο να καταβάλει στον Επίτροπο Πληροφοριών το ποσό που καθορίζεται στην ειδοποίηση. Ειδοποίηση επιβολής κυρώσεων μπορεί να εκδοθεί σε περίπτωση μη συμμόρφωσης με ορισμένες διατάξεις του DPA 2018 ([174]) ή να απευθυνθεί σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία που δεν συμμορφώθηκε με ειδοποίηση παροχής πληροφοριών, ειδοποίηση διενέργειας αξιολόγησης ή ειδοποίηση επιβολής μέτρων.

(103) Ειδικότερα, προκειμένου να καθοριστεί αν ο Επίτροπος Πληροφοριών θα απευθύνει ειδοποίηση επιβολής κυρώσεων σε υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία αλλά και για να καθοριστεί το ύψος της ποινής, ο Επίτροπος Πληροφοριών πρέπει να λαμβάνει υπόψη τα θέματα που απαριθμούνται στο άρθρο 155 παράγραφος 3 του DPA 2018, μεταξύ άλλων τη φύση και τη σοβαρότητα της μη συμμόρφωσης, τον εκ προθέσεως ή εξ αμελείας χαρακτήρα της μη συμμόρφωσης, τυχόν ενέργειες στις οποίες προέβη ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία για τον μετριασμό της ζημίας που υπέστησαν τα υποκείμενα των δεδομένων, τον βαθμό ευθύνης του υπευθύνου επεξεργασίας ή

([168]) Παράρτημα 13 παράγραφος 2 του DPA 2018.
([169]) Άρθρο 142 του DPA 2018 (υπό την επιφύλαξη των περιορισμών του άρθρου 143 του DPA 2018).
([170]) Άρθρο 146 του DPA 2018 (υπό την επιφύλαξη των περιορισμών του άρθρου 147 του DPA 2018).
([171]) Άρθρα 149 έως 151 του DPA 2018 (υπό την επιφύλαξη των περιορισμών του άρθρου 152 του DPA 2018).
([172]) Άρθρο 155 του DPA 2018 (υπό την επιφύλαξη των περιορισμών του άρθρου 156 του DPA 2018).
([173]) Regulatory Action Policy, διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf.
([174]) Ειδικότερα, το ICO μπορεί να εκδώσει ειδοποίηση επιβολής κυρώσεων για μη συμμόρφωση, όπως προβλέπεται στο άρθρο 149 παράγραφοι 2, 3, 4 ή 5 του DPA 2018.

του εκτελούντος την επεξεργασία (λαμβανομένων υπόψη των τεχνικών και οργανωτικών μέτρων που εφαρμόζει ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία), τυχόν σχετικές προηγούμενες περιπτώσεις μη συμμόρφωσης του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία· τις κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζονται από τη μη συμμόρφωση και το αν η κύρωση θα ήταν αποτελεσματική, αναλογική και αποτρεπτική.

(104) Το μέγιστο ποσό της ποινής που μπορεί να επιβληθεί μέσω ειδοποίησης επιβολής κυρώσεων είναι α) 17 500 000 λίρες στερλίνες (GBP) όσον αφορά τη μη συμμόρφωση με τις αρχές προστασίας των δεδομένων (άρθρα 35, 36, 37, 38 παράγραφος 1, 39 παράγραφος 1 και άρθρο 40 του DPA 2018), τις υποχρεώσεις διαφάνειας και τα ατομικά δικαιώματα (άρθρα 44, 45, 46, 47, 48, 49, 52 και 53 του DPA 2018), καθώς και τις αρχές για τις διεθνείς διαβιβάσεις δεδομένων προσωπικού χαρακτήρα (άρθρα 73, 75, 76, 77 ή 78 του DPA 2018)· και β) σε άλλη περίπτωση, 8 700 000 GBP ([175]). Όσον αφορά μη συμμόρφωση με ειδοποίηση παροχής πληροφοριών, ειδοποίηση διενέργειας αξιολόγησης ή ειδοποίηση επιβολής μέτρων, το μέγιστο ποσό της ποινής που μπορεί να επιβληθεί μέσω ειδοποίησης επιβολής κυρώσεων ανέρχεται σε 17 500 000 GBP.

(105) Σύμφωνα με τις τελευταίες ετήσιες εκθέσεις της (2018-2019 ([176]), 2019-2020 ([177])), η Επίτροπος Πληροφοριών έχει διεξαγάγει σειρά ερευνών όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις αρχές επιβολής του ποινικού δικαίου. Για παράδειγμα, η Επίτροπος διεξήγαγε έρευνα και δημοσίευσε γνώμη τον Οκτώβριο του 2019 σχετικά με τη χρήση της τεχνολογίας αναγνώρισης προσώπου από τις αρχές επιβολής του νόμου σε δημόσιους χώρους. Η έρευνα επικεντρώθηκε ειδικότερα στη χρήση των δυνατοτήτων ζωντανής αναγνώρισης προσώπου από την αστυνομία της Νότιας Ουαλίας και τη Μητροπολιτική Αστυνομία (Metropolitan Police Service, MPS). Επιπλέον, η Επίτροπος διερεύνησε τον «Κατάλογο συμμοριών» (Gangs matrix) ([178]) της MPS και διαπίστωσε σειρά σοβαρών παραβάσεων της νομοθεσίας για την προστασία των δεδομένων που ήταν πιθανό να υπονομεύσουν την εμπιστοσύνη του κοινού στο εν λόγω εργαλείο και τη χρήση των δεδομένων.

(106) Τον Νοέμβριο του 2018 η νυν επίτροπος Πληροφοριών εξέδωσε ειδοποίηση επιβολής μέτρων και, στη συνέχεια, η MPS έλαβε τα απαιτούμενα μέτρα για την αύξηση της ασφάλειας και της λογοδοσίας, αλλά και για τη διασφάλιση της αναλογικής χρήσης των δεδομένων.

(107) Άλλο παράδειγμα πρόσφατης επιβολής είναι το πρόστιμο των 325 000 GBP που επέβαλε η νυν επίτροπος τον Μάιο του 2018 σε βάρος της Εισαγγελικής Αρχής του Στέμματος, για την απώλεια μη κρυπτογραφημένων DVD που περιείχαν ηχογραφήσεις καταθέσεων στην αστυνομία. Επιπλέον, η νυν επίτροπος Πληροφοριών διεξήγαγε έρευνες για ευρύτερα θέματα, όπως για παράδειγμα, κατά το πρώτο εξάμηνο του 2020, έρευνα σχετικά με τη χρήση της εξαγωγής δεδομένων από κινητά τηλέφωνα στο πλαίσιο της αστυνόμευσης και την επεξεργασία δεδομένων θυμάτων από την αστυνομία.

(108) Εκτός από τις εν λόγω εξουσίες επιβολής του επιτρόπου Πληροφοριών, ορισμένες παραβάσεις της νομοθεσίας για την προστασία των δεδομένων συνιστούν αδικήματα και ενδέχεται, ως εκ τούτου, να υπόκεινται σε ποινικές κυρώσεις (άρθρο 196 του DPA 2018). Αυτό ισχύει, για παράδειγμα, για τη λήψη ή την κοινολόγηση δεδομένων προσωπικού χαρακτήρα χωρίς τη συγκατάθεση του υπευθύνου επεξεργασίας και για την παροχή της κοινολόγησης δεδομένων προσωπικού χαρακτήρα σε άλλο πρόσωπο χωρίς τη συγκατάθεση του υπευθύνου επεξεργασίας ([179])· για την επαναταυτοποίηση πληροφοριών που αποτελούν αποταυτοποιημένα δεδομένα προσωπικού χαρακτήρα χωρίς τη συγκατάθεση του υπεύθυνου για την αποταυτοποίηση των δεδομένων προσωπικού χαρακτήρα υπευθύνου επεξεργασίας ([180])· για τη με πρόθεση παρακώλυση της άσκησης των εξουσιών του Επιτρόπου όσον αφορά την επιθεώρηση δεδομένων προσωπικού χαρακτήρα σύμφωνα με διεθνείς υποχρεώσεις ([181]), την υποβολή ψευδών δηλώσεων σε απάντηση σε ειδοποίηση παροχής πληροφοριών ή την καταστροφή πληροφοριών σε σχέση με ειδοποιήσεις παροχής πληροφοριών και διενέργειας αξιολόγησης ([182]).

(109) Ο Επίτροπος Πληροφοριών έχει επίσης καθήκον, σύμφωνα με το άρθρο 139 του DPA 2018, να υποβάλλει σε κάθε σώμα του Κοινοβουλίου γενική έκθεση σχετικά με την άσκηση των καθηκόντων του βάσει του νόμου ([183]).

([175]) Άρθρο 157 του DPA 2018.

([176]) Information Commissioner's Annual Report and Financial Statements 2018-2019, διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf.

([177]) Information Commissioner's Annual Report 2019-2020 (βλέπε υποσημείωση 157).

([178]) Βάση δεδομένων στην οποία καταγράφονται πληροφορίες σχετικά με φερόμενα μέλη συμμοριών και θύματα εγκλημάτων που σχετίζονται με συμμορίες.

([179]) Άρθρο 170 του DPA 2018.

([180]) Άρθρο 171 του DPA 2018.

([181]) Άρθρο 119 του DPA 2018.

([182]) Άρθρα 144 και 148 του DPA 2018.

([183]) Όπως ορίζεται στη συμφωνία διαχείρισης, η ετήσια έκθεση πρέπει: i) να καλύπτει όλες τις επιχειρήσεις, θυγατρικές ή κοινοπραξίες που τελούν υπό τον έλεγχο του ICO· ii) να συμμορφώνεται με το Εγχειρίδιο Χρηματοοικονομικής Πληροφόρησης του υπουργείου Οικονομικών (Financial Reporting Manual, FReM)· iii) να περιέχει δήλωση διακυβέρνησης, στην οποία καθορίζονται οι τρόποι με τους οποίους ο υπόλογος διαχειρίστηκε και έλεγξε τους πόρους που χρησιμοποιήθηκαν στον οργανισμό κατά τη διάρκεια του έτους, καταδεικνύοντας πόσο καλά διαχειρίζεται ο οργανισμός τους κινδύνους για την επίτευξη των σκοπών και των στόχων του· και iv) να περιγράφει τις κύριες δραστηριότητες και επιδόσεις κατά τη διάρκεια του προηγούμενου οικονομικού έτους και να παρουσιάζει συνοπτικά τα μελλοντικά σχέδια (Management Agreement 2018-2021, παράγραφος 3.26, βλέπε υποσημείωση 158).

2.5.2. *Εποπτεία του δικαστικού σώματος*

(110) Η εποπτεία της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα δικαστήρια και το δικαστικό σώμα είναι διττή. Όταν ένας κάτοχος δικαστικού αξιώματος ή ένα δικαστήριο δεν ενεργεί στο πλαίσιο της δικαιοδοτικής του αρμοδιότητας, η εποπτεία διασφαλίζεται από τον Επίτροπο Πληροφοριών. Όταν ο υπεύθυνος επεξεργασίας ενεργεί στο πλαίσιο της δικαιοδοτικής του αρμοδιότητας, το ICO δεν μπορεί να ασκεί τα εποπτικά του καθήκοντα ([184]) και η εποπτεία διενεργείται από ειδικούς φορείς. Αυτό αντικατοπτρίζει την προσέγγιση που ακολουθείται στο άρθρο 32 της οδηγίας (ΕΕ) 2016/680.

(111) Ειδικότερα, στη δεύτερη περίπτωση, όσον αφορά τα δικαστήρια της Αγγλίας και της Ουαλίας και τα πρωτοδικεία διοικητικών διαφορών (First-tier Tribunals) και τα εφετεία διοικητικών διαφορών (Upper Tribunals) της Αγγλίας και της Ουαλίας, η εν λόγω εποπτεία παρέχεται από την Ειδική Ομάδα Προστασίας Δικαστικών Δεδομένων (Judicial Data Protection Panel) ([185]). Επιπλέον, ο λόρδος αρχιδικαστής (Lord Chief Justice) και ο ανώτατος πρόεδρος των ειδικών δικαιοδοτικών οργάνων (Senior President of Tribunals) εξέδωσαν δήλωση περί προστασίας της ιδιωτικότητας ([186]), στην οποία περιγράφεται ο τρόπος με τον οποίο τα δικαστήρια της Αγγλίας και της Ουαλίας επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα για την άσκηση δικαστικών καθηκόντων. Παρόμοια δήλωση έχει εκδοθεί από το δικαστικό σώμα της Βόρειας Ιρλανδίας ([187]) και της Σκωτίας ([188]).

(112) Επιπλέον, στη Βόρεια Ιρλανδία, ο λόρδος αρχιδικαστής της Βόρειας Ιρλανδίας έχει διορίσει δικαστή του Ανώτερου Δικαστηρίου (High Court) ως δικαστή εποπτείας δεδομένων (Data Supervisory Judge, DSJ) ([189]). Έχει επίσης εκδώσει οδηγίες προς το δικαστικό σώμα της Βόρειας Ιρλανδίας σχετικά με τις ενέργειες που πρέπει να πραγματοποιούνται σε περίπτωση απώλειας ή δυνητικής απώλειας δεδομένων και τη διαδικασία αντιμετώπισης τυχόν ζητημάτων που προκύπτουν συναφώς ([190]).

(113) Στη Σκωτία, ο Λόρδος πρόεδρος (Lord President) έχει διορίσει έναν δικαστή εποπτείας δεδομένων για τη διερεύνηση τυχόν καταγγελιών για λόγους προστασίας των δεδομένων. Ο εν λόγω διορισμός προβλέπεται από τους κανόνες για τις δικαστικές καταγγελίες, που αντικατοπτρίζουν εκείνους που θεσπίστηκαν για την Αγγλία και την Ουαλία ([191]).

(114) Τέλος, στο Ανώτατο Δικαστήριο (Supreme Court), διορίζεται ένας από τους δικαστές του Ανώτατου Δικαστηρίου για την εποπτεία της προστασίας των δεδομένων.

([184]) Άρθρο 117 του DPA 2018.

([185]) Η ειδική ομάδα είναι αρμόδια για την παροχή καθοδήγησης και κατάρτισης στο δικαστικό σώμα. Ασχολείται επίσης με καταγγελίες από υποκείμενα δεδομένων σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από δικαστήρια, δικαιοδοτικά όργανα και φυσικά πρόσωπα που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας. Στόχος της ειδικής ομάδας είναι να παρέχει τα μέσα με τα οποία θα μπορούσε να επιλυθεί κάθε καταγγελία. Εάν ένας καταγγέλλων δεν είναι ικανοποιημένος με απόφαση της ειδικής ομάδας και προσκομίσει πρόσθετα αποδεικτικά στοιχεία, η ειδική ομάδα θα μπορούσε να επανεξετάσει την απόφασή της. Μολονότι η ίδια η ειδική ομάδα δεν επιβάλλει οικονομικές κυρώσεις, εάν κρίνει όμως ότι υπάρχει κατάφωρη παράβαση του DPA 2018, μπορεί να την παραπέμψει στην Υπηρεσία Διερεύνησης Καταγγελιών κατά Δικαστικών Λειτουργών (Judicial Conduct Investigation Office, JCIO), η οποία θα διερευνήσει την καταγγελία. Εάν η καταγγελία γίνει δεκτή, εναπόκειται στον υπουργό Δικαιοσύνης (Lord Chancellor) και στον Λόρδο Αρχιδικαστή (ή σε ανώτερο δικαστή που έχει εξουσιοδοτηθεί να ενεργεί εξ ονόματός του) να αποφασίσουν ποια μέτρα πρέπει να ληφθούν κατά του κατόχου δικαστικού αξιώματος. Αυτά θα μπορούσαν να περιλαμβάνουν, κατά σειρά σοβαρότητας: επίσημη συμβουλή, επίσημη προειδοποίηση και επίπληξη, καθώς και, εντέλει, παύση από τα καθήκοντα. Εάν ένα πρόσωπο δεν είναι ικανοποιημένο με τον τρόπο με τον οποίο διερευνήθηκε η καταγγελία από την JCIO, μπορεί να υποβάλει επίσης καταγγελία στον διαμεσολαβητή για τους διορισμούς δικαστικών και τη δικαστική δεοντολογία (Judicial Appointments and Conduct Ombudsman) (βλέπε https://www.gov.uk/government/organisations/judicial-appointments-and-conduct-ombudsman). Ο διαμεσολαβητής έχει την εξουσία να ζητήσει από την JCIO να διερευνήσει εκ νέου μια καταγγελία και μπορεί να προτείνει την καταβολή αποζημίωσης στον καταγγέλλοντα όταν θεωρεί ότι έχει υποστεί ζημία ως αποτέλεσμα κακοδιοίκησης.

([186]) Η δήλωση περί προστασίας της ιδιωτικότητας του λόρδου αρχιδικαστή και του ανώτατου προέδρου των ειδικών δικαιοδοτικών οργάνων είναι διαθέσιμη στον ακόλουθο σύνδεσμο: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([187]) Η δήλωση περί ιδιωτικότητας του Λόρδου Αρχιδικαστή της Βόρειας Ιρλανδίας διατίθεται στον ακόλουθο σύνδεσμο: https://judiciaryni.uk/data-privacy.

([188]) Η δήλωση περί προστασίας της ιδιωτικότητας για τα δικαστήρια και τα δικαιοδοτικά όργανα της Σκωτίας διατίθεται στον ακόλουθο σύνδεσμο: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice.

([189]) Ο δικαστής εποπτείας δεδομένων παρέχει καθοδήγηση στο δικαστικό σώμα και διερευνά παραβάσεις και/ή καταγγελίες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από δικαστήρια ή φυσικά πρόσωπα που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας.

([190]) Όταν η καταγγελία ή η παράβαση θεωρείται σοβαρή, παραπέμπεται στον υπεύθυνο δικαστικών καταγγελιών (Judicial Complaints Officer) για περαιτέρω διερεύνηση σύμφωνα με τον κώδικα ορθής πρακτικής του Λόρδου Αρχιδικαστή της Βόρειας Ιρλανδίας σχετικά με τις καταγγελίες. Η έκβαση μιας τέτοιας καταγγελίας θα μπορούσε να περιλαμβάνει: καμία περαιτέρω ενέργεια, συμβουλή, κατάρτιση ή καθοδήγηση, άτυπη προειδοποίηση, επίσημη προειδοποίηση, τελική προειδοποίηση, περιορισμός άσκησης καθηκόντων ή παραπομπή σε νόμιμο δικαιοδοτικό όργανο. Ο κώδικας ορθής πρακτικής του Λόρδου Αρχιδικαστή της Βόρειας Ιρλανδίας σχετικά με τις καταγγελίες διατίθεται στον ακόλουθο σύνδεσμο: https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf.

([191]) Κάθε καταγγελία που είναι βάσιμη διερευνάται από τον δικαστή εποπτείας δεδομένων και παραπέμπεται στον Λόρδο Πρόεδρο ο οποίος έχει την εξουσία να εκδίδει συμβουλή, επίσημη προειδοποίηση ή επίπληξη εφόσον το κρίνει αναγκαίο (ισοδύναμοι κανόνες ισχύουν για τα μέλη των δικαιοδοτικών οργάνων και διατίθενται στον ακόλουθο σύνδεσμο: https://www.judiciary.scot/docs/librariesprovider3/judiciary documents/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2).

2.5.3. *Μέσα προσφυγής*

(115) Για να διασφαλίζεται επαρκής προστασία και ειδικότερα η επιβολή των ατομικών δικαιωμάτων, το υποκείμενο των δεδομένων πρέπει να έχει στη διάθεσή του αποτελεσματικά μέσα διοικητικής και δικαστικής προσφυγής, συμπεριλαμβανομένης της αποζημίωσης.

(116) Πρώτον, το υποκείμενο των δεδομένων έχει το δικαίωμα να υποβάλει καταγγελία στον Επίτροπο Πληροφοριών εάν θεωρεί ότι έχει υπάρξει παράβαση του μέρους 3 του DPA 2018, σε σχέση με δεδομένα προσωπικού χαρακτήρα που το αφορούν ([192]). Όπως περιγράφεται στις αιτιολογικές σκέψεις (100) και (109), ο Επίτροπος Πληροφοριών έχει την εξουσία να αξιολογεί τη συμμόρφωση του υπευθύνου επεξεργασίας και του εκτελούντος την επεξεργασία με τον DPA 2018, να τους υποχρεώνει να λαμβάνουν αναγκαία μέτρα σε περίπτωση μη συμμόρφωσης ή να απέχουν από τη λήψη μέτρων και να επιβάλλει πρόστιμα.

(117) Δεύτερον, ο DPA 2018 παρέχει δικαίωμα προσφυγής κατά του Επιτρόπου Πληροφοριών. Εάν ο Επίτροπος δεν «προωθήσει» ([193]) τη διεκπεραίωση καταγγελίας που έχει υποβληθεί από το υποκείμενο των δεδομένων, ο καταγγέλλων έχει δικαίωμα δικαστικής προσφυγής, καθώς μπορεί να υποβάλει αίτηση σε πρωτοδικείο διοικητικών διαφορών ([194]) για να διατάξει τον Επίτροπο να λάβει τα κατάλληλα μέτρα ώστε να απαντήσει στην καταγγελία ή να ενημερώσει τον καταγγέλλοντα σχετικά με την πρόοδο της καταγγελίας ([195]). Επιπλέον, κάθε πρόσωπο το οποίο λαμβάνει από τον Επίτροπο οποιαδήποτε από τις ανωτέρω ειδοποιήσεις (παροχής πληροφοριών, διενέργειας αξιολόγησης, επιβολής μέτρων ή επιβολής κυρώσεων) μπορεί να προσφύγει ενώπιον πρωτοδικείου διοικητικών διαφορών. Εάν το δικαστήριο κρίνει ότι η απόφαση του Επιτρόπου δεν είναι σύμφωνη με τον νόμο ή ότι ο Επίτροπος Πληροφοριών θα έπρεπε να είχε ασκήσει τη διακριτική του ευχέρεια με διαφορετικό τρόπο, το δικαστήριο πρέπει να κάνει δεκτή την προσφυγή ή να αντικαταστήσει την ειδοποίηση με άλλη ειδοποίηση ή απόφαση που θα μπορούσε να είχε απευθύνει ή να είχε εκδώσει ο Επίτροπος Πληροφοριών ([196]).

(118) Τρίτον, τα φυσικά πρόσωπα μπορούν να ασκήσουν δικαστική προσφυγή κατά υπευθύνων επεξεργασίας και εκτελούντων την επεξεργασία προσφεύγοντας απευθείας ενώπιον των δικαστηρίων σύμφωνα με το άρθρο 167 του DPA 2018. Εάν, κατόπιν αίτησης του υποκειμένου των δεδομένων, το δικαστήριο κρίνει ότι υπήρξε παραβίαση των δικαιωμάτων του εν λόγω υποκειμένου των δεδομένων βάσει της νομοθεσίας για την προστασία των δεδομένων, το δικαστήριο μπορεί να διατάξει τον υπεύθυνο επεξεργασίας, ή τον εκτελούντα την επεξεργασία που ενεργεί για λογαριασμό του εν λόγω υπευθύνου επεξεργασίας, να λάβει τα μέτρα που προσδιορίζονται στη διαταγή ή να μην προβεί στη λήψη των μέτρων που προσδιορίζονται στη διαταγή. Επιπλέον, σύμφωνα με το άρθρο 169 του DPA 2018, κάθε πρόσωπο που υφίσταται ζημία λόγω παραβίασης απαίτησης της νομοθεσίας για την προστασία των δεδομένων (συμπεριλαμβανομένου του μέρους 3 του DPA 2018), εκτός από τον ΓΚΠΔ του Ηνωμένου Βασιλείου, δικαιούται αποζημίωση για τη ζημία αυτή από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία, εκτός εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία αποδείξει ότι ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δεν ευθύνεται με κανέναν τρόπο για το γεγονός που προκάλεσε τη ζημία. Η ζημία περιλαμβάνει τόσο την οικονομική ζημία όσο και τη μη οικονομική ζημία, όπως την πρόκληση οδύνης.

(119) Τέταρτον, εφόσον οποιοδήποτε πρόσωπο θεωρεί ότι τα δικαιώματά του, συμπεριλαμβανομένων των δικαιωμάτων στην προστασία της ιδιωτικότητας και των δεδομένων, έχουν παραβιαστεί από δημόσιες αρχές, μπορεί να προσφύγει ενώπιον των δικαστηρίων του Ηνωμένου Βασιλείου βάσει του νόμου του 1998 για τα ανθρώπινα δικαιώματα. Οι υπεύθυνοι επεξεργασίας δυνάμει του μέρους 3 του DPA 2018, δηλαδή οι αρμόδιες αρχές, είναι πάντοτε δημόσιες αρχές κατά την έννοια του νόμου του 1998 για τα ανθρώπινα δικαιώματα. Ένα φυσικό πρόσωπο που ισχυρίζεται ότι μια δημόσια αρχή ενήργησε (ή προτίθεται να ενεργήσει) κατά τρόπο ασυμβίβαστο με δικαίωμα της σύμβασης, και κατά συνέπεια παράνομο δυνάμει του άρθρου 6 παράγραφος 1 του νόμου του 1998 για τα ανθρώπινα δικαιώματα, μπορεί να ασκήσει προσφυγή κατά της αρχής ενώπιον του αρμόδιου δικαστηρίου ή δικαιοδοτικού οργάνου, ή να επικαλεστεί τα σχετικά δικαιώματα σε οποιαδήποτε δικαστική διαδικασία, εφόσον είναι (ή θα ήταν) θύμα της παράνομης πράξης ([197]).

([192]) Άρθρο 165 του DPA 2018.

([193]) Το άρθρο 166 του DPA 2018 αναφέρεται ρητά στις ακόλουθες περιπτώσεις: α) ο Επίτροπος δεν λαμβάνει τα κατάλληλα μέτρα για να απαντήσει στην καταγγελία, β) ο Επίτροπος δεν παρέχει στον καταγγέλλοντα πληροφορίες σχετικά με την πρόοδο της καταγγελίας ή την έκβαση της καταγγελίας, πριν από το τέλος της περιόδου 3 μηνών που αρχίζει με την παραλαβή της καταγγελίας από τον Επίτροπο, ή γ) εάν η εξέταση της καταγγελίας από τον Επίτροπο δεν ολοκληρωθεί εντός της εν λόγω περιόδου, δεν παρέχει στον καταγγέλλοντα τις πληροφορίες αυτές εντός επακόλουθης περιόδου 3 μηνών.

([194]) Το πρωτοδικείο διοικητικών διαφορών είναι το αρμόδιο για την εξέταση προσφυγών κατά αποφάσεων που λαμβάνονται από κρατικούς ρυθμιστικούς φορείς. Στην περίπτωση απόφασης του Επιτρόπου Πληροφοριών, αρμόδιο είναι το τμήμα Γενικής Αρμοδιότητας (General Regulatory Chamber), το οποίο έχει δικαιοδοσία σε ολόκληρο το Ηνωμένο Βασίλειο.

([195]) Άρθρο 166 του DPA 2018.

([196]) Άρθρα 161 και 162 του DPA 2018.

([197]) Βλέπε υπόθεση Brown κατά Commissioner of the Met 2016, όπου το δικαστήριο παρείχε επανόρθωση στην ενάγουσα στο πλαίσιο της προστασίας δεδομένων σε αγωγή που ασκήθηκε κατά της αστυνομίας. Το δικαστήριο αποφάνθηκε υπέρ της ενάγουσας, κάνοντας δεκτούς τους ισχυρισμούς της σχετικά με την παράβαση των υποχρεώσεων δυνάμει του DPA 1998, την παράβαση του νόμου του 1998 για τα ανθρώπινα δικαιώματα (και του σχετικού δικαιώματος του άρθρου 8 της ΕΣΔΑ) και της αδικοπραξίας για κατάχρηση ιδιωτικών πληροφοριών (ο εναγόμενος παραδέχθηκε τελικά ότι παρέβη τον νόμο για την προστασία των δεδομένων και την ΕΣΔΑ, οπότε η απόφαση επικεντρώθηκε στο ερώτημα ποιο είδος έννομης προστασίας ήταν κατάλληλο). Ως αποτέλεσμα των παραβάσεων αυτών, το δικαστήριο επιδίκασε χρηματική αποζημίωση στην ενάγουσα.

(120) Εάν το δικαστήριο διαπιστώσει ότι οποιαδήποτε πράξη δημόσιας αρχής είναι παράνομη, μπορεί να χορηγήσει τη σχετική επανόρθωση ή αποκατάσταση, ή να εκδώσει τη διαταγή, στο πλαίσιο των αρμοδιοτήτων του, που κρίνει δίκαιη και κατάλληλη ([198]). Το δικαστήριο μπορεί επίσης να κηρύξει διάταξη πρωτογενούς δικαίου ασυμβίβαστη με δικαίωμα που διασφαλίζεται από την ΕΣΔΑ.

(121) Τέλος, αφού εξαντλήσει τα εθνικά ένδικα μέσα, ένα πρόσωπο μπορεί να προσφύγει ενώπιον του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου για παραβιάσεις των δικαιωμάτων που κατοχυρώνονται στην ΕΣΔΑ.

2.6. **Περαιτέρω κοινοποίηση**

(122) Το δίκαιο του Ηνωμένου Βασιλείου επιτρέπει την κοινοποίηση δεδομένων από αρχή επιβολής του νόμου σε άλλες αρχές του Ηνωμένου Βασιλείου για σκοπούς διαφορετικούς από εκείνους για τους οποίους συλλέχθηκαν αρχικά (η λεγόμενη «περαιτέρω κοινοποίηση») υπό ορισμένες προϋποθέσεις.

(123) Όπως προβλέπεται και στο άρθρο 4 παράγραφος 2 της οδηγίας (ΕΕ) 2016/680, το άρθρο 36 παράγραφος 3 του DPA 2018 επιτρέπει την περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα που συλλέχθηκαν από αρμόδια αρχή για σκοπούς επιβολής του νόμου (είτε από τον αρχικό υπεύθυνο επεξεργασίας είτε από άλλον υπεύθυνο επεξεργασίας) για οποιονδήποτε άλλο σκοπό επιβολής του νόμου, υπό την προϋπόθεση ότι ο υπεύθυνος επεξεργασίας είναι εκ του νόμου εξουσιοδοτημένος να επεξεργάζεται δεδομένα για τον εν λόγω άλλο σκοπό και ότι η επεξεργασία είναι αναγκαία και αναλογική ([199]). Στην περίπτωση αυτή, όλες οι εγγυήσεις που προβλέπονται στο μέρος 3 του DPA 2018 και οι οποίες αναλύονται ανωτέρω έχουν εφαρμογή στην επεξεργασία που διενεργείται από την αποδέκτρια αρχή.

(124) Στην έννομη τάξη του Ηνωμένου Βασιλείου, η περαιτέρω κοινοποίηση επιτρέπεται ρητά από διάφορους νόμους. Ειδικότερα, i) ο νόμος του 2017 για την ψηφιακή οικονομία (Digital Economy Act 2017) επιτρέπει την ανταλλαγή δεδομένων μεταξύ δημόσιων αρχών για διάφορους σκοπούς, για παράδειγμα στην περίπτωση απάτης σε βάρος του δημόσιου τομέα η οποία συνεπάγεται ζημία ή κίνδυνο ζημίας για δημόσιες αρχές ([200]) ή σε περίπτωση χρέους προς δημόσια αρχή ή προς το Στέμμα ([201])· ii) ο νόμος του 2013 για τη δίωξη του εγκλήματος και τα δικαστήρια επιτρέπει την κοινοποίηση πληροφοριών στην Εθνική Υπηρεσία Δίωξης του Εγκλήματος (NCA) ([202]) με σκοπό την καταπολέμηση, τη διερεύνηση και τη δίωξη του σοβαρού και οργανωμένου εγκλήματος· iii) ο νόμος του 2007 για τη δίωξη σοβαρών εγκλημάτων (Serious Crime Act 2007) επιτρέπει στις δημόσιες αρχές να κοινολογούν πληροφορίες σε οργανισμούς καταπολέμησης της απάτης με σκοπό την πρόληψη της απάτης ([203]).

(125) Οι νόμοι αυτοί προβλέπουν ρητά ότι η κοινοποίηση πληροφοριών θα πρέπει να πραγματοποιείται σύμφωνα με τους κανόνες που καθορίζονται στον DPA 2018. Επιπλέον, το Σώμα των Εργαζομένων στην Αστυνόμευση έχει εκδώσει εγκεκριμένη επαγγελματική πρακτική σχετικά με την κοινοποίηση πληροφοριών ([204]) προκειμένου να συνδράμει την αστυνομία στη συμμόρφωση με τις υποχρεώσεις της όσον αφορά την προστασία δεδομένων βάσει του ΓΚΠΔ του Ηνωμένου Βασιλείου, του νόμου για την προστασία των δεδομένων και του νόμου του 1998 για τα ανθρώπινα δικαιώματα. Η συμμόρφωση της κοινοποίησης με το ισχύον νομικό πλαίσιο για την προστασία των δεδομένων μπορεί να υπόκειται, φυσικά, σε δικαστικό έλεγχο ([205]).

(126) Επιπλέον, όπως προβλέπεται και στο άρθρο 9 της οδηγίας (ΕΕ) 2016/680, ο DPA 2018 προβλέπει ότι τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται για οποιονδήποτε σκοπό επιβολής του νόμου μπορούν να υποβάλλονται σε επεξεργασία για σκοπό που δεν ανάγεται στην επιβολή του νόμου, αν η επεξεργασία επιτρέπεται από τον νόμο ([206]). Αυτού του είδους η κοινοποίηση καλύπτει δύο σενάρια: 1) την περίπτωση στην οποία μια αρχή επιβολής του ποινικού δικαίου κοινοποιεί δεδομένα σε αρχή επιβολής του νόμου σε τομείς πέραν του ποινικού δικαίου η οποία δεν είναι υπηρεσία

([198]) Άρθρο 8 παράγραφος 1 του νόμου του 1998 για τα ανθρώπινα δικαιώματα.

([199]) Άρθρο 36 παράγραφος 3 του DPA 2018.

([200]) Άρθρο 56 του νόμου του 2017 για την ψηφιακή οικονομία, διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2017/30/contents.

([201]) Άρθρο 48 του νόμου του 2017 για την ψηφιακή οικονομία.

([202]) Άρθρο 7 του νόμου του 2013 για τη δίωξη του εγκλήματος και τα δικαστήρια, διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2013/22/contents.

([203]) Άρθρο 68 του νόμου του 2007 για τη δίωξη σοβαρών εγκλημάτων, διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2007/27/contents.

([204]) Authorised Professional Practice on Information Sharing, διατίθεται στον ακόλουθο σύνδεσμο: https://www.app.college.police.uk/app-content/information-management/sharing-police-information.

([205]) Βλέπε, για παράδειγμα, υπόθεση M κατά Chief Constable of Sussex Police [2019] EWHC 975 (Admin), στην οποία το Ανώτερο Δικαστήριο κλήθηκε να εξετάσει την ανταλλαγή δεδομένων μεταξύ της αστυνομίας και μιας σύμπραξης για τη μείωση του εταιρικού εγκλήματος (Business Crime Reduction Partnership, BCRP), οργανισμού ο οποίος είναι εξουσιοδοτημένος να διαχειρίζεται το σύστημα ειδοποίησης αποκλεισμού, με το οποίο απαγορεύεται η είσοδος προσώπων στις εμπορικές εγκαταστάσεις των μελών του. Το δικαστήριο εξέτασε την ανταλλαγή δεδομένων, η οποία πραγματοποιήθηκε βάσει συμφωνίας με σκοπό την προστασία του κοινού και την πρόληψη του εγκλήματος, και κατέληξε εντέλει στο συμπέρασμα ότι οι περισσότερες πτυχές της ανταλλαγής δεδομένων ήταν νόμιμες, με εξαίρεση ορισμένες ευαίσθητες πληροφορίες που ανταλλάχθηκαν μεταξύ της αστυνομίας και της BCRP. Άλλο παράδειγμα είναι η υπόθεση Cooper κατά NCA [2019] EWCA Civ 16, στην οποία το Εφετείο (Court of Appeal) έκρινε νόμιμη την ανταλλαγή δεδομένων μεταξύ της αστυνομίας και της Υπηρεσίας Δίωξης Σοβαρού Οργανωμένου Εγκλήματος (Serious Organised Crime Agency, SOCA), μιας υπηρεσίας επιβολής του νόμου που αποτελεί επί του παρόντος μέρος της NCA.

([206]) Άρθρο 36 παράγραφος 4 του DPA 2018.

πληροφοριών (όπως π.χ. οικονομική ή φορολογική αρχή, αρχή ανταγωνισμού, υπηρεσία κοινωνικής μέριμνας για τους νέους)· 2) την περίπτωση στην οποία μια αρχή επιβολής του ποινικού δικαίου κοινοποιεί δεδομένα σε υπηρεσία πληροφοριών. Στο πρώτο σενάριο, η επεξεργασία δεδομένων προσωπικού χαρακτήρα εμπίπτει στο πεδίο εφαρμογής του ΓΚΠΔ του Ηνωμένου Βασιλείου, καθώς και στο μέρος 2 του DPA 2018. Όπως προσδιορίζεται στην απόφαση που εκδόθηκε δυνάμει του κανονισμού (ΕΕ) 2016/679, οι εγγυήσεις που προβλέπονται από τον ΓΚΠΔ του Ηνωμένου Βασιλείου και το μέρος 2 του DPA 2018 παρέχουν επίπεδο προστασίας το οποίο είναι κατ' ουσίαν ισοδύναμο με εκείνο που παρέχεται εντός της Ένωσης ([207]).

(127) Στο δεύτερο σενάριο, όσον αφορά την κοινοποίηση δεδομένων που συλλέγονται από αρχή επιβολής του ποινικού δικαίου σε υπηρεσία πληροφοριών για σκοπούς εθνικής ασφάλειας, η νομική βάση που επιτρέπει την εν λόγω κοινοποίηση είναι ο νόμος του 2008 για την καταπολέμηση της τρομοκρατίας (Counter Terrorism Act, CTA 2008) ([208]). Σύμφωνα με τον CTA 2008, κάθε πρόσωπο μπορεί να παρέχει πληροφορίες σε οποιαδήποτε από τις υπηρεσίες πληροφοριών με σκοπό την εκπλήρωση οποιουδήποτε από τα καθήκοντα της εν λόγω υπηρεσίας, συμπεριλαμβανομένης της «εθνικής ασφάλειας».

(128) Όσον αφορά τις προϋποθέσεις υπό τις οποίες μπορούν να κοινοποιούνται δεδομένα για σκοπούς εθνικής ασφάλειας, ο νόμος για τις υπηρεσίες πληροφοριών (Intelligence Services Act) και ο νόμος για την Υπηρεσία Ασφάλειας (Security Service Act) περιορίζουν τη δυνατότητα των υπηρεσιών πληροφοριών να λαμβάνουν δεδομένα σε ό,τι είναι αναγκαίο για την εκπλήρωση των εκ του νόμου καθηκόντων τους. Οι αρμόδιες αρχές που εμπίπτουν στο πεδίο εφαρμογής του μέρους 3 του DPA 2018 και επιδιώκουν την κοινοποίηση δεδομένων στις υπηρεσίες πληροφοριών θα πρέπει να εξετάσουν διάφορους παράγοντες/περιορισμούς επιπλέον των εκ του νόμου καθηκόντων των υπηρεσιών τα οποία καθορίζονται στον νόμο για τις υπηρεσίες πληροφοριών και στον νόμο για την Υπηρεσία Ασφάλειας ([209]). Το άρθρο 20 του CTA 2008 ορίζει σαφώς ότι κάθε κοινοποίηση δεδομένων που πραγματοποιείται σύμφωνα με το άρθρο 19 του CTA 2008 πρέπει να συμμορφώνεται με τη νομοθεσία για την προστασία των δεδομένων· αυτό σημαίνει ότι ισχύουν όλοι οι περιορισμοί και οι απαιτήσεις του DPA 2018. Επιπλέον, οι αρχές επιβολής του νόμου και οι υπηρεσίες πληροφοριών είναι δημόσιες αρχές για τους σκοπούς του νόμου του 1998 για τα ανθρώπινα δικαιώματα και, ως εκ τούτου, πρέπει να διασφαλίζουν ότι ενεργούν σύμφωνα με τα δικαιώματα που κατοχυρώνονται στην ΕΣΔΑ, συμπεριλαμβανομένου του άρθρου 8. Με άλλα λόγια, οι απαιτήσεις αυτές σημαίνουν ότι κάθε ανταλλαγή δεδομένων μεταξύ των υπηρεσιών επιβολής του νόμου και των υπηρεσιών πληροφοριών συμμορφώνεται με τη νομοθεσία για την προστασία των δεδομένων και την ΕΣΔΑ.

(129) Η επεξεργασία —από τις υπηρεσίες πληροφοριών— των δεδομένων προσωπικού χαρακτήρα που λαμβάνονται ή αποκτώνται από τις αρχές επιβολής του νόμου για σκοπούς εθνικής ασφάλειας υπόκειται σε ορισμένες προϋποθέσεις και εγγυήσεις ([210]). Το μέρος 4 του DPA 2018 εφαρμόζεται σε κάθε επεξεργασία που πραγματοποιείται από τις υπηρεσίες

([207]) Εκτελεστική απόφαση της Επιτροπής σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με την επάρκεια της παρεχόμενης από το Ηνωμένο Βασίλειο προστασίας των δεδομένων προσωπικού χαρακτήρα [C(2021)4800].

([208]) Άρθρο 19 του νόμου του 2008 για την καταπολέμηση της τρομοκρατίας, διατίθεται στον ακόλουθο σύνδεσμο: https://www.legislation.gov.uk/ukpga/2008/28/section/19.

([209]) Το άρθρο 2 παράγραφος 2 του νόμου του 1994 για τις υπηρεσίες πληροφοριών (βλέπε https://www.legislation.gov.uk/ukpga/1994/13/contents) προβλέπει ότι «Ο διοικητής της Υπηρεσίας Πληροφοριών είναι υπεύθυνος για την αποτελεσματικότητα της εν λόγω υπηρεσίας και έχει καθήκον να διασφαλίζει— α) ότι υπάρχουν ρυθμίσεις που εξασφαλίζουν ότι η Υπηρεσία Πληροφοριών δεν λαμβάνει πληροφορίες παρά μόνο στον βαθμό που είναι αναγκαίο για την ορθή εκτέλεση των καθηκόντων της και ότι δεν κοινολογεί καμία πληροφορία παρά μόνο στον βαθμό που είναι αναγκαίο— i) για τον σκοπό αυτόν· ii) προς το συμφέρον της εθνικής ασφάλειας· iii) για τον σκοπό της πρόληψης ή της ανίχνευσης σοβαρών εγκλημάτων· ή iv) για τους σκοπούς οποιασδήποτε ποινικής διαδικασίας· και β) ότι η Υπηρεσία Πληροφοριών δεν προβαίνει σε καμία ενέργεια για την προώθηση των συμφερόντων οποιουδήποτε πολιτικού κόμματος του Ηνωμένου Βασιλείου», ενώ το άρθρο 2 παράγραφος 2 του νόμου του 1989 για την Υπηρεσία Ασφάλειας (βλέπε https://www.legislation.gov.uk/ukpga/1989/5/contents) προβλέπει ότι «Ο γενικός διευθυντής είναι υπεύθυνος για την αποτελεσματικότητα της Υπηρεσίας και έχει καθήκον να διασφαλίζει — α) ότι υπάρχουν ρυθμίσεις που διασφαλίζουν ότι η Υπηρεσία δεν λαμβάνει πληροφορίες παρά μόνο στον βαθμό που είναι αναγκαίο για την ορθή εκτέλεση των καθηκόντων της, ούτε τις κοινολογεί παρά μόνο στον βαθμό που είναι αναγκαίο για τον σκοπό αυτό ή για τους σκοπούς της πρόληψης ή της ανίχνευσης σοβαρών εγκλημάτων ή για τον σκοπό οποιασδήποτε ποινικής διαδικασίας· και β) ότι η Υπηρεσία δεν προβαίνει σε καμία ενέργεια για την προώθηση των συμφερόντων οποιουδήποτε πολιτικού κόμματος· και γ) ότι υπάρχουν ρυθμίσεις, οι οποίες συμφωνούνται με τον γενικό διευθυντή της Εθνικής Υπηρεσίας Δίωξης του Εγκλήματος, για τον συντονισμό των δραστηριοτήτων της Υπηρεσίας σύμφωνα με το άρθρο 1 παράγραφος 4 του παρόντος νόμου σχετικά με τις δραστηριότητες των αστυνομικών δυνάμεων, της Εθνικής Υπηρεσίας Δίωξης του Εγκλήματος και άλλων υπηρεσιών επιβολής του νόμου».

([210]) Οι εγγυήσεις και οι περιορισμοί σε σχέση με τις εξουσίες των υπηρεσιών πληροφοριών ρυθμίζονται επίσης από τον νόμο του 2016 για τις ερευνητικές εξουσίες, ο οποίος, σε συνδυασμό με τον νόμο του 2000 για τη ρύθμιση των ερευνητικών εξουσιών για την Αγγλία, την Ουαλία και τη Βόρεια Ιρλανδία και τον νόμο του 2000 για τη ρύθμιση των ερευνητικών εξουσιών (Σκωτία) για τη Σκωτία, προβλέπει τη νομική βάση για τη χρήση των εν λόγω εξουσιών. Ωστόσο, οι εξουσίες αυτές δεν είναι συναφείς στο πλαίσιο της «περαιτέρω κοινοποίησης», δεδομένου ότι καλύπτουν την άμεση συλλογή δεδομένων προσωπικού χαρακτήρα από τις υπηρεσίες πληροφοριών. Για την αξιολόγηση των εξουσιών που ανατίθενται στις υπηρεσίες πληροφοριών δυνάμει του νόμου για τις ερευνητικές εξουσίες, βλέπε την εκτελεστική απόφαση της Επιτροπής σύμφωνα με τον κανονισμό (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, σχετικά με την επάρκεια της παρεχόμενης από το Ηνωμένο Βασίλειο προστασίας των δεδομένων προσωπικού χαρακτήρα [C(2021) 4800].

πληροφοριών ή για λογαριασμό τους. Καθορίζει τις βασικές αρχές προστασίας των δεδομένων (νομιμότητα, αντικειμενικότητα και διαφάνεια ([211])· περιορισμός του σκοπού ([212])· ελαχιστοποίηση των δεδομένων ([213])· ακρίβεια ([214])· περιορισμός περιόδου αποθήκευσης ([215]) και ασφάλεια ([216])), επιβάλλει προϋποθέσεις για την επεξεργασία δεδομένων ειδικών κατηγοριών ([217]), προβλέπει τα δικαιώματα του υποκειμένου των δεδομένων ([218]), απαιτεί την προστασία δεδομένων από τον σχεδιασμό και εξ ορισμού ([219]) και ρυθμίζει τις διεθνείς διαβιβάσεις των δεδομένων προσωπικού χαρακτήρα ([220]).

(130) Ταυτόχρονα, το άρθρο 110 του DPA 2018 προβλέπει εξαίρεση από την εφαρμογή συγκεκριμένων διατάξεων του μέρους 4 του DPA 2018, όταν η εξαίρεση αυτή απαιτείται για τη διαφύλαξη της εθνικής ασφάλειας. Το άρθρο 110 παράγραφος 2 του DPA 2018 απαριθμεί τις διατάξεις από την εφαρμογή των οποίων επιτρέπεται εξαίρεση. Περιλαμβάνει τις αρχές προστασίας των δεδομένων (εκτός από την αρχή της νομιμότητας), τα δικαιώματα του υποκειμένου των δεδομένων, την υποχρέωση ενημέρωσης του Επιτρόπου Πληροφοριών σχετικά με παραβίαση δεδομένων, τις εξουσίες επιθεώρησης του Επιτρόπου Πληροφοριών σύμφωνα με τις διεθνείς υποχρεώσεις, ορισμένες από τις εξουσίες επιβολής του Επιτρόπου Πληροφοριών, τις διατάξεις που καθιστούν ορισμένες παραβιάσεις της προστασίας δεδομένων ποινικό αδίκημα, καθώς και τις διατάξεις που αφορούν ειδικούς σκοπούς επεξεργασίας, όπως δημοσιογραφικούς, ακαδημαϊκούς ή καλλιτεχνικούς σκοπούς. Η εξαίρεση αυτή μπορεί να βασίζεται σε κατά περίπτωση ανάλυση ([221]). Όπως εξήγησαν οι αρχές του Ηνωμένου Βασιλείου και επιβεβαιώνεται από τη νομολογία των δικαστηρίων του Ηνωμένου Βασιλείου, «ο υπεύθυνος επεξεργασίας πρέπει να εξετάζει τις πραγματικές συνέπειες για την εθνική ασφάλεια ή άμυνα εάν χρειαζόταν να συμμορφωθεί με τη συγκεκριμένη διάταξη περί προστασίας των δεδομένων και εάν θα μπορούσε ευλόγως να συμμορφωθεί με τον συνήθη κανόνα χωρίς να θίγεται η εθνική ασφάλεια ή άμυνα» ([222]). Το αν η εξαίρεση έχει χρησιμοποιηθεί κατάλληλα ή όχι υπόκειται στην εποπτεία του ICO ([223]).

([211]) Σύμφωνα με το άρθρο 86 παράγραφος 6 του DPA 2018, για τον προσδιορισμό της αντικειμενικότητας και της διαφάνειας της επεξεργασίας, πρέπει να λαμβάνεται υπόψη η μέθοδος με την οποία λαμβάνονται τα δεδομένα. Υπό την έννοια αυτή, η απαίτηση αντικειμενικότητας και διαφάνειας πληρούται εάν τα δεδομένα λαμβάνονται από πρόσωπο το οποίο έχει νομίμως εξουσιοδοτηθεί ή υποχρεούται να τα παράσχει.

([212]) Σύμφωνα με το άρθρο 87 του DPA 2018, οι σκοποί της επεξεργασίας πρέπει να είναι καθορισμένοι, ρητοί και νόμιμοι. Τα δεδομένα δεν πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο ασύμβατο με τους σκοπούς για τους οποίους συλλέγονται. Σύμφωνα με το άρθρο 87 παράγραφος 3 του ίδιου νόμου, η περαιτέρω συμβατή επεξεργασία δεδομένων προσωπικού χαρακτήρα μπορεί να επιτρέπεται μόνον εάν ο υπεύθυνος επεξεργασίας είναι εξουσιοδοτημένος από τον νόμο να επεξεργάζεται τα δεδομένα για τον σκοπό αυτό και η επεξεργασία είναι αναγκαία και αναλογική προς τον εν λόγω σκοπό. Η επεξεργασία θα πρέπει να θεωρείται συμβατή, εάν συνίσταται σε επεξεργασία για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς, και υπόκειται σε κατάλληλες εγγυήσεις (άρθρο 87 παράγραφος 4 του DPA 2018).

([213]) Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή και όχι υπερβολικά (άρθρο 88 του DPA 2018).

([214]) Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι ακριβή και επικαιροποιημένα (άρθρο 89 του DPA 2018).

([215]) Τα δεδομένα προσωπικού χαρακτήρα δεν πρέπει να διατηρούνται για μεγαλύτερο χρονικό διάστημα απ' ό,τι είναι αναγκαίο (άρθρο 90 του DPA 2018).

([216]) Η έκτη αρχή προστασίας των δεδομένων είναι ότι τα δεδομένα προσωπικού χαρακτήρα πρέπει να υποβάλλονται σε επεξεργασία κατά τρόπο που να περιλαμβάνει τη λήψη κατάλληλων μέτρων ασφαλείας όσον αφορά τους κινδύνους που προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι κίνδυνοι περιλαμβάνουν (μεταξύ άλλων) την τυχαία ή μη εξουσιοδοτημένη πρόσβαση σε δεδομένα προσωπικού χαρακτήρα ή την καταστροφή, την απώλεια, τη χρήση, την τροποποίηση ή την κοινολόγησή τους (άρθρο 91 του DPA 2018). Το άρθρο 107 ορίζει επίσης ότι 1) κάθε υπεύθυνος επεξεργασίας πρέπει να εφαρμόζει κατάλληλα μέτρα ασφαλείας ανάλογα με τους κινδύνους που προκύπτουν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και 2) στην περίπτωση αυτοματοποιημένης επεξεργασίας, κάθε υπεύθυνος επεξεργασίας και κάθε εκτελών την επεξεργασία εφαρμόζει μέτρα πρόληψης ή μετριασμού βάσει αξιολόγησης του κινδύνου.

([217]) Άρθρο 86 παράγραφος 2 στοιχείο b) και παράρτημα 10 του DPA 2018.

([218]) Μέρος 4 κεφάλαιο 3 του DPA 2018, κυρίως τα δικαιώματα: πρόσβασης, διόρθωσης και διαγραφής, αντίταξης στην επεξεργασία και μη υπαγωγής σε αυτοματοποιημένη λήψη αποφάσεων, παρέμβασης στην αυτοματοποιημένη λήψη αποφάσεων και ενημέρωσης σχετικά με τη λήψη αποφάσεων. Επιπλέον, ο υπεύθυνος επεξεργασίας πρέπει να παρέχει στο υποκείμενο των δεδομένων πληροφορίες σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

([219]) Άρθρο 103 του DPA 2018.

([220]) Άρθρο 109 του DPA 2018. Οι διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε διεθνείς οργανισμούς ή χώρες εκτός του Ηνωμένου Βασιλείου είναι δυνατές εάν η διαβίβαση αποτελεί αναγκαίο και αναλογικό μέτρο που διενεργείται για τους σκοπούς των εκ του νόμου καθηκόντων του υπευθύνου επεξεργασίας ή για άλλους σκοπούς που προβλέπονται σε συγκεκριμένα άρθρα του νόμου του 1989 για την Υπηρεσία Ασφάλειας και του νόμου του 1994 για τις υπηρεσίες πληροφοριών.

([221]) Βλέπε υπόθεση Baker κατά Secretary of State for the Home Department [2001] UKIT NSA2 (στο εξής: Baker κατά Secretary of State).

([222]) UK Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework, σ. 15-16, διατίθεται στον ακόλουθο σύνδεσμο https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Βλέπε επίσης Baker v Secretary of State (βλέπε ανωτέρω υποσημείωση 220),, στην οποία το δικαστήριο ακύρωσε πιστοποιητικό εθνικής ασφάλειας το οποίο εξέδωσε ο υπουργός Εσωτερικών και επιβεβαίωσε την εφαρμογή της εξαίρεσης εθνικής ασφάλειας, κρίνοντας ότι δεν υπήρχε λόγος να προβλεφθεί εξαίρεση γενικού χαρακτήρα από την υποχρέωση απάντησης σε αιτήματα πρόσβασης και ότι η χορήγηση της εξαίρεσης αυτής σε όλες τις περιπτώσεις —χωρίς κατά περίπτωση ανάλυση— υπερέβαινε αυτό που ήταν αναγκαίο και αναλογικό για την προστασία της εθνικής ασφάλειας.

([223]) Βλέπε μνημόνιο συμφωνίας μεταξύ του ICO και της Κοινότητας Πληροφοριών του Ηνωμένου Βασιλείου (UK Intelligence Community, UKIC) σύμφωνα με το οποίο: «Με την υποβολή καταγγελίας από υποκείμενο των δεδομένων, το ICO θα επιδιώξει να πειστεί ότι το ζήτημα έχει αντιμετωπιστεί ορθά και, κατά περίπτωση, ότι η εφαρμογή τυχόν εξαίρεσης έχει χρησιμοποιηθεί κατάλληλα» (Memorandum of Understanding between Information Commissioner's Office and the UK Intelligence Community, παράγραφος 16, διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf).

(131) Επιπλέον, όσον αφορά τη δυνατότητα περιορισμού οποιουδήποτε από τα προαναφερόμενα δικαιώματα για την προστασία της «εθνικής ασφάλειας», το άρθρο 79 του DPA 2018 προβλέπει ότι ο υπεύθυνος επεξεργασίας μπορεί να υποβάλει αίτηση για πιστοποιητικό υπογεγραμμένο από υπουργό ή από τον γενικό εισαγγελέα, το οποίο να πιστοποιεί ότι ο περιορισμός των εν λόγω δικαιωμάτων αποτελεί, ή σε οποιαδήποτε στιγμή αποτέλεσε, αναγκαίο και αναλογικό μέτρο για την προστασία της εθνικής ασφάλειας ([224]). Η κυβέρνηση του Ηνωμένου Βασιλείου έχει εκδώσει οδηγίες σχετικά με τα πιστοποιητικά εθνικής ασφάλειας στο πλαίσιο του DPA 2018, στις οποίες επισημαίνεται κυρίως ότι κάθε περιορισμός των δικαιωμάτων των υποκειμένων των δεδομένων για τη διαφύλαξη της εθνικής ασφάλειας πρέπει να είναι αναλογικός και αναγκαίος ([225]). Όλα τα πιστοποιητικά εθνικής ασφάλειας πρέπει να δημοσιεύονται στον δικτυακό τόπο του ICO ([226]).

(132) Το πιστοποιητικό θα πρέπει να έχει καθορισμένη διάρκεια που να μην υπερβαίνει τα πέντε έτη, ώστε να επανεξετάζεται τακτικά από τον υπουργό ([227]). Το πιστοποιητικό προσδιορίζει τα δεδομένα προσωπικού χαρακτήρα ή τις κατηγορίες δεδομένων προσωπικού χαρακτήρα που υπόκεινται στην εξαίρεση, καθώς και τις διατάξεις του DPA 2018 στις οποίες εφαρμόζεται η εξαίρεση ([228]).

(133) Είναι σημαντικό να σημειωθεί ότι τα πιστοποιητικά εθνικής ασφάλειας δεν παρέχουν πρόσθετο λόγο για τον περιορισμό των δικαιωμάτων προστασίας των δεδομένων για λόγους εθνικής ασφάλειας. Με άλλα λόγια, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία μπορεί να βασίζεται σε πιστοποιητικό μόνον εφόσον έχει καταλήξει στο συμπέρασμα ότι είναι αναγκαίο να βασιστεί στην εξαίρεση της εθνικής ασφάλειας, η οποία πρέπει να εφαρμόζεται κατά περίπτωση. Ακόμη και αν ένα πιστοποιητικό εθνικής ασφάλειας εφαρμόζεται στο υπό εξέταση ζήτημα, το ICO μπορεί να διερευνήσει αν η επίκληση της εξαίρεσης της εθνικής ασφάλειας ήταν δικαιολογημένη σε συγκεκριμένη υπόθεση ([229]).

(134) Κάθε πρόσωπο που θίγεται άμεσα από την έκδοση του πιστοποιητικού μπορεί να προσφύγει στο εφετείο διοικητικών διαφορών ([230]) κατά του πιστοποιητικού ([231]) ή, όταν το πιστοποιητικό προσδιορίζει δεδομένα μέσω γενικής περιγραφής, να αμφισβητήσει την εφαρμογή του πιστοποιητικού σε συγκεκριμένα δεδομένα ([232]).

(135) Το δικαστήριο επανεξετάζει την απόφαση έκδοσης πιστοποιητικού και αποφασίζει αν υπήρχαν βάσιμοι λόγοι για την έκδοση του πιστοποιητικού ([233]). Μπορεί να εξετάζει ευρύ φάσμα θεμάτων, συμπεριλαμβανομένης της αναγκαιότητας, της αναλογικότητας και της νομιμότητας, λαμβάνοντας υπόψη τον αντίκτυπο στα δικαιώματα των υποκειμένων των δεδομένων και σταθμίζοντας την ανάγκη διαφύλαξης της εθνικής ασφάλειας. Ως εκ τούτου, το δικαστήριο μπορεί να αποφασίσει ότι το πιστοποιητικό δεν εφαρμόζεται σε συγκεκριμένα δεδομένα προσωπικού χαρακτήρα που αποτελούν το αντικείμενο της προσφυγής ([234]).

([224]) Ο DPA 2018 κατάργησε τη δυνατότητα έκδοσης πιστοποιητικού βάσει του άρθρου 28 παράγραφος 2 του νόμου του 1998 για την προστασία των δεδομένων. Ωστόσο, η δυνατότητα έκδοσης «παλαιών πιστοποιητικών» εξακολουθεί να υφίσταται στον βαθμό που υπάρχει ιστορική προσφυγή βάσει του νόμου του 1998 (βλέπε παράρτημα 20 μέρος 5 παράγραφος 17 του DPA 2018). Ωστόσο, η εφαρμογή της δυνατότητας αυτής φαίνεται πολύ σπάνια και θα εφαρμόζεται μόνο σε περιορισμένες περιπτώσεις, όπως, για παράδειγμα, όταν ένα υποκείμενο δεδομένων προσφεύγει κατά της χρήσης της εξαίρεσης της εθνικής ασφάλειας σε σχέση με επεξεργασία από δημόσια αρχή που έχει πραγματοποιήσει την επεξεργασία βάσει του νόμου του 1998. Πρέπει να σημειωθεί ότι στις περιπτώσεις αυτές το άρθρο 28 του DPA 1998 θα εφαρμόζεται στο σύνολό του, συμπεριλαμβανομένης, ως εκ τούτου, της δυνατότητας του υποκειμένου των δεδομένων να προσβάλει το πιστοποιητικό. Επί του παρόντος δεν υπάρχει πιστοποιητικό εθνικής ασφάλειας που να έχει εκδοθεί βάσει του DPA 1998.

([225]) UK Government Guidance on National Security Certificates under the Data Protection Act 2018, διατίθεται στον ακόλουθο σύνδεσμο: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

([226]) Σύμφωνα με το άρθρο 130 του DPA 2018, το ICO μπορεί να αποφασίσει να μη δημοσιεύσει το κείμενο ή μέρος του κειμένου του πιστοποιητικού, εάν η δημοσίευση αντίκειται στο συμφέρον της εθνικής ασφάλειας ή αντίκειται στο δημόσιο συμφέρον ή ενδέχεται να θέσει σε κίνδυνο την ασφάλεια οποιουδήποτε προσώπου. Στις περιπτώσεις αυτές, ωστόσο, το ICO δημοσιεύει το γεγονός ότι το πιστοποιητικό έχει εκδοθεί.

([227]) UK Government Guidance on National Security Certificates, παράγραφος 15, βλέπε υποσημείωση 225.

([228]) UK Government Guidance on National Security Certificates, παράγραφος 5, βλέπε υποσημείωση 224.

([229]) Το άρθρο 102 του DPA 2018 απαιτεί ο υπεύθυνος επεξεργασίας να είναι σε θέση να αποδείξει ότι έχει συμμορφωθεί με τον DPA 2018. Αυτό σημαίνει ότι μια υπηρεσία πληροφοριών θα πρέπει να αποδείξει στο ICO ότι, όταν βασίζεται στην εξαίρεση, έχει λάβει υπόψη τις ειδικές περιστάσεις της υπόθεσης. Το ICO δημοσιεύει επίσης αρχείο των πιστοποιητικών εθνικής ασφάλειας, το οποίο διατίθεται στον ακόλουθο σύνδεσμο: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/.

([230]) Το εφετείο διοικητικών διαφορών είναι το δικαστήριο που είναι αρμόδιο να εκδικάζει εφέσεις κατά αποφάσεων κατώτερων διοικητικών δικαστηρίων και έχει ειδική αρμοδιότητα για τις απευθείας προσφυγές κατά αποφάσεων ορισμένων κυβερνητικών οργάνων.

([231]) Άρθρο 111 παράγραφος 3 του DPA 2018.

([232]) Άρθρο 111 παράγραφος 5 του DPA 2018.

([233]) Στην υπόθεση Baker κατά Secretary of State (βλέπε υποσημείωση 221), το Ειδικό Δικαιοδοτικό Όργανο Υποθέσεων Πληροφοριών (Information Tribunal) ακύρωσε πιστοποιητικό εθνικής ασφάλειας το οποίο εξέδωσε ο υπουργός Εσωτερικών, κρίνοντας ότι δεν υπήρχε λόγος να προβλεφθεί εξαίρεση γενικού χαρακτήρα από την υποχρέωση απάντησης σε αιτήματα πρόσβασης και ότι η χορήγηση της εξαίρεσής αυτής σε όλες τις περιπτώσεις, χωρίς κατά περίπτωση ανάλυση, υπερέβαινε το αναγκαίο και αναλογικό για την προστασία της εθνικής ασφάλειας.

([234]) UK Government Guidance on National Security Certificates, παράγραφος 25, βλέπε υποσημείωση 225.

(136) Ένα διαφορετικό σύνολο πιθανών περιορισμών αφορά εκείνους που εφαρμόζονται, σύμφωνα με το παράρτημα 11 του DPA 2018, σε ορισμένες διατάξεις του μέρους 4 του DPA 2018 ([235]) για τη διασφάλιση άλλων σημαντικών σκοπών γενικού δημόσιου συμφέροντος ή προστατευόμενων συμφερόντων, όπως, για παράδειγμα, τα κοινοβουλευτικά προνόμια, το δικηγορικό απόρρητο, η διεξαγωγή δικαστικών διαδικασιών ή το αξιόμαχο των ενόπλων δυνάμεων. Η εξαίρεση από την εφαρμογή των διατάξεων αυτών προβλέπεται είτε για ορισμένες κατηγορίες πληροφοριών («βάσει κατηγορίας») είτε στον βαθμό που η εφαρμογή των εν λόγω διατάξεων είναι πιθανό να θίξει το προστατευόμενο συμφέρον («βάσει ζημίας») ([236]). Επίκληση εξαιρέσεων βάσει ζημίας είναι δυνατή μόνον εφόσον η εφαρμογή της παρατιθέμενης διάταξης για την προστασία των δεδομένων είναι πιθανό να θίξει το συγκεκριμένο συμφέρον. Ως εκ τούτου, η χρήση εξαίρεσης πρέπει πάντοτε να αιτιολογείται με αναφορά στη σχετική ζημία που θα ήταν πιθανό να προκύψει στη συγκεκριμένη περίπτωση. Η επίκληση εξαιρέσεων βάσει κατηγοριών μπορεί να πραγματοποιηθεί μόνο σε σχέση με τη συγκεκριμένη, στενά καθορισμένη κατηγορία πληροφοριών για την οποία χορηγείται η εξαίρεση. Οι εξαιρέσεις αυτές είναι παρόμοιες —ως προς τον σκοπό και τις επιπτώσεις τους— με αρκετές από τις εξαιρέσεις του ΓΚΠΔ του Ηνωμένου Βασιλείου (σύμφωνα με το παράρτημα 2 του DPA 2018), οι οποίες, με τη σειρά τους, αντικατοπτρίζουν εκείνες που προβλέπονται στο άρθρο 23 του ΓΚΠΔ.

(137) Από τα ανωτέρω συνάγεται ότι ο περιορισμός και οι προϋποθέσεις ισχύουν βάσει των εφαρμοστέων νομικών διατάξεων του Ηνωμένου Βασιλείου, όπως ερμηνεύονται επίσης από τα δικαστήρια και το Γραφείο Επιτρόπου Πληροφοριών, ώστε να διασφαλίζεται ότι η εν λόγω εξαίρεση και οι εν λόγω περιορισμοί παραμένουν εντός των ορίων της αναγκαιότητας και της αναλογικότητας για την προστασία της εθνικής ασφάλειας.

(138) Η επεξεργασία δεδομένων προσωπικού χαρακτήρα που διενεργείται από τις υπηρεσίες πληροφοριών δυνάμει του μέρους 4 του DPA 2018 τελεί υπό την εποπτεία του Επιτρόπου Πληροφοριών ([237]).

(139) Τα γενικά καθήκοντα του Επιτρόπου Πληροφοριών σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις υπηρεσίες πληροφοριών δυνάμει του μέρους 4 του DPA 2018 καθορίζονται στο παράρτημα 13 του εν λόγω νόμου. Στα καθήκοντα περιλαμβάνονται, μεταξύ άλλων, ειδικότερα, η παρακολούθηση και η επιβολή του μέρους 4 του DPA 2018, η προώθηση της ευαισθητοποίησης του κοινού, η παροχή συμβουλών στο Κοινοβούλιο, στην κυβέρνηση και σε άλλα όργανα όσον αφορά νομοθετικά και διοικητικά μέτρα, η προώθηση της ευαισθητοποίησης των υπευθύνων επεξεργασίας και των εκτελούντων την επεξεργασία σχετικά με τις υποχρεώσεις τους, η παροχή πληροφοριών στο υποκείμενο των δεδομένων σχετικά με την άσκηση των δικαιωμάτων του και η διεξαγωγή ερευνών.

(140) Όπως και για το μέρος 3 του DPA 2018, ο Επίτροπος έχει την εξουσία να ενημερώνει τους υπευθύνους επεξεργασίας σχετικά με εικαζόμενη παράβαση και να εκδίδει προειδοποιήσεις επισημαίνοντας ότι μια πράξη επεξεργασίας είναι πιθανόν να παραβαίνει τους κανόνες, καθώς και να απευθύνει επίπληξη σε περίπτωση που επιβεβαιωθεί η παράβαση. Μπορεί επίσης να εκδίδει ειδοποιήσεις επιβολής μέτρων και ειδοποιήσεις επιβολής κυρώσεων για παραβάσεις ορισμένων διατάξεων του νόμου ([238]). Ωστόσο, σε αντίθεση με όσα ισχύουν για άλλα μέρη του DPA 2018, ο Επίτροπος δεν μπορεί να απευθύνει ειδοποίηση διενέργειας αξιολόγησης σε φορέα εθνικής ασφάλειας ([239]).

(141) Επιπλέον, το άρθρο 110 του DPA 2018 προβλέπει εξαίρεση σε σχέση με την άσκηση ορισμένων εξουσιών του Επιτρόπου, όταν αυτό απαιτείται για τους σκοπούς της διαφύλαξης της εθνικής ασφάλειας. Αυτό περιλαμβάνει την εξουσία του Επιτρόπου να εκδίδει (οποιουδήποτε είδους) ειδοποιήσεις δυνάμει του DPA (ειδοποιήσεις παροχής πληροφοριών, διενέργειας αξιολόγησης, επιβολής μέτρων και επιβολής κυρώσεων), την εξουσία διενέργειας επιθεωρήσεων σύμφωνα με τις

([235]) Σ' αυτές περιλαμβάνονται: i) οι αρχές του μέρους 4 για την προστασία των δεδομένων, εκτός από την απαίτηση νομιμότητας της επεξεργασίας βάσει της πρώτης αρχής και το γεγονός ότι η επεξεργασία πρέπει να πληροί μία από τις σχετικές προϋποθέσεις που ορίζονται στα παραρτήματα 9 και 10· ii) τα δικαιώματα των υποκειμένων των δεδομένων· και iii) τα καθήκοντα που σχετίζονται με την καταγγελία παραβάσεων στο ICO.

([236]) Σύμφωνα με το επεξηγηματικό πλαίσιο του Ηνωμένου Βασιλείου (UK Explanatory Framework), οι εξαιρέσεις «βάσει κατηγορίας» είναι οι εξής: i) οι πληροφορίες σχετικά με την απονομή τιμητικών τίτλων του Στέμματος· ii) το δικηγορικό απόρρητο· iii) οι εμπιστευτικές πληροφορίες σχετικά με την απασχόληση, την κατάρτιση ή την εκπαίδευση· και iv) τα γραπτά και οι βαθμολογίες εξετάσεων. Οι εξαιρέσεις «βάσει ζημίας» αφορούν τα ακόλουθα θέματα: i) πρόληψη ή ανίχνευση εγκλημάτων· σύλληψη και δίωξη παραβατών· ii) κοινοβουλευτικά προνόμια· iii) δικαστικές διαδικασίες· iv) το αξιόμαχο των ενόπλων δυνάμεων του Στέμματος· v) την οικονομική ευημερία του Ηνωμένου Βασιλείου· vi) διαπραγματεύσεις με το υποκείμενο των δεδομένων· vii) επιστημονική ή ιστορική έρευνα ή στατιστικούς σκοπούς· viii) αρχειοθέτηση προς το δημόσιο συμφέρον. UK Explanatory Framework for Adequacy Discussions, section H: National Security, σ. 13, βλέπε υποσημείωση 222.

([237]) Άρθρο 116 του DPA 2018.

([238]) Σύμφωνα με συνδυαστική ανάγνωση του άρθρου 149 παράγραφος 2 και του άρθρου 155 του DPA 2018, μπορούν να εκδίδονται ειδοποιήσεις επιβολής μέτρων και ειδοποιήσεις επιβολής κυρώσεων προς υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία για παραβάσεις του μέρους 4 κεφάλαιο 2 του DPA 2018 (αρχές της επεξεργασίας), διάταξης του μέρους 4 του DPA 2018 που παρέχει δικαιώματα σε υποκείμενο δεδομένων, της απαίτησης κοινοποίησης παραβίασης δεδομένων προσωπικού χαρακτήρα στον Επίτροπο σύμφωνα με το άρθρο 108 του DPA 2018, και των αρχών που διέπουν τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, χώρες που δεν είναι συμβαλλόμενα μέρη της σύμβασης και διεθνείς οργανισμούς δυνάμει του άρθρου 109 του DPA 2018. [Για περισσότερες λεπτομέρειες σχετικά με την ειδοποίηση επιβολής μέτρων και την ειδοποίηση επιβολής κυρώσεων, βλέπε αιτιολογικές σκέψεις (102) έως (103)].

([239]) Σύμφωνα με το άρθρο 147 παράγραφος 6 του DPA 2018, ο Επίτροπος Πληροφοριών δεν μπορεί να απευθύνει ειδοποίηση διενέργειας αξιολόγησης σε φορέα που καθορίζεται στο άρθρο 23 παράγραφος 3 του νόμου του 2000 για την ελευθερία της πληροφόρησης (Freedom of Information Act 2000). Σ' αυτούς περιλαμβάνεται η Υπηρεσία Ασφάλειας (MI5), η Μυστική Υπηρεσία Πληροφοριών (MI6) και η Κεντρική Κυβερνητική Υπηρεσία Επικοινωνιών.

διεθνείς υποχρεώσεις, τις εξουσίες εισόδου και διενέργειας επιθεώρησης και τους κανόνες που αφορούν τα ποινικά αδικήματα ([240]). Όπως εξηγείται στην αιτιολογική σκέψη (136), οι εξαιρέσεις αυτές θα εφαρμόζονται μόνον εφόσον είναι αναγκαίες και αναλογικές και μόνο κατά περίπτωση. Η εφαρμογή αυτών των εξαιρέσεων μπορεί να υπόκειται σε δικαστικό έλεγχο ([241]).

(142) Το ICO και οι υπηρεσίες πληροφοριών του Ηνωμένου Βασιλείου έχουν υπογράψει μνημόνιο συμφωνίας ([242]) με το οποίο θεσπίζεται πλαίσιο συνεργασίας για διάφορα θέματα, συμπεριλαμβανομένων των γνωστοποιήσεων παραβιάσεων δεδομένων και του χειρισμού των καταγγελιών των υποκειμένων των δεδομένων. Ειδικότερα, το εν λόγω μνημόνιο συμφωνίας προβλέπει ότι το ICO, μόλις λάβει καταγγελία, θα αξιολογεί αν έχει γίνει κατάλληλη επίκληση οποιασδήποτε εξαίρεσης εθνικής ασφάλειας. Οι απαντήσεις σε ερωτήματα που υποβάλλονται από το ICO στο πλαίσιο της εξέτασης μεμονωμένων καταγγελιών πρέπει να παρέχονται εντός 20 εργάσιμων ημερών με βάση τις σχετικές οδηγίες της κυβέρνησης του Ηνωμένου Βασιλείου σχετικά με τα πιστοποιητικά εθνικής ασφάλειας δυνάμει του νόμου για την προστασία των δεδομένων (UK Government Guidance on National Security Certificates under the Data Protection Act), με χρήση κατάλληλων ασφαλών διαύλων εάν πρόκειται για διαβαθμισμένες πληροφορίες. Από τον Απρίλιο του 2018 έως σήμερα, το ICO έχει λάβει 21 καταγγελίες προσώπων οι οποίες αφορούσαν τις υπηρεσίες πληροφοριών. Όλες οι καταγγελίες εξετάστηκαν και το αποτέλεσμα κοινοποιήθηκε στο υποκείμενο των δεδομένων ([243]).

(143) Επιπλέον, η Επιτροπή Πληροφοριών και Ασφάλειας (Intelligence and Security Committee, ISC) ασκεί την κοινοβουλευτική εποπτεία της επεξεργασίας δεδομένων από τις υπηρεσίες πληροφοριών. Η εν λόγω επιτροπή αντλεί τη νομική της βάση από τον νόμο του 2013 για τη δικαιοσύνη και την ασφάλεια (Justice and Security Act, JSA 2013) ([244]). Με τον νόμο αυτό συστάθηκε η ISC ως επιτροπή του Κοινοβουλίου του Ηνωμένου Βασιλείου. Η ISC αποτελείται από μέλη που ανήκουν σε οποιοδήποτε από τα δύο σώματα του Κοινοβουλίου και διορίζονται από τον πρωθυπουργό αφού ζητηθεί η γνώμη του αρχηγού της αντιπολίτευσης ([245]). Η ISC υποχρεούται να υποβάλλει στο Κοινοβούλιο ετήσια έκθεση σχετικά με την εκτέλεση των καθηκόντων της, καθώς και άλλες εκθέσεις που θεωρεί σκόπιμο να υποβληθούν ([246]).

(144) Από το 2013 έχουν ανατεθεί στην ISC ευρύτερες εξουσίες, συμπεριλαμβανομένης της εποπτείας των επιχειρησιακών δραστηριοτήτων των υπηρεσιών ασφάλειας. Σύμφωνα με το άρθρο 2 του JSA 2013, η ISC έχει καθήκον να επιβλέπει τις δαπάνες, τη διοίκηση, την πολιτική και τις επιχειρήσεις των υπηρεσιών εθνικής ασφάλειας. Ο JSA 2013 ορίζει ότι η ISC έχει τη δυνατότητα να διεξάγει έρευνες επί επιχειρησιακών θεμάτων, όταν δεν σχετίζονται με επιχειρήσεις που βρίσκονται σε

([240]) Οι διατάξεις από την εφαρμογή των οποίων χωρεί εξαίρεση είναι: το άρθρο 108 (κοινοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στον Επίτροπο), το άρθρο 119 (επιθεώρηση σύμφωνα με τις διεθνείς υποχρεώσεις)· τα άρθρα 142 έως 154 και το παράρτημα 15 (ειδοποιήσεις του Επιτρόπου και εξουσίες εισόδου και διενέργειας επιθεώρησης)· και τα άρθρα 170 έως 173 (αδικήματα σχετικά με δεδομένα προσωπικού χαρακτήρα). Επιπλέον, όσον αφορά την επεξεργασία από τις υπηρεσίες πληροφοριών, στο παράρτημα 13 (άλλα γενικά καθήκοντα του Επιτρόπου), η παράγραφος 1 στοιχεία a) και g) και η παράγραφος 2.

([241]) Βλέπε για παράδειγμα υπόθεση Baker κατά Secretary of State for the Home Department (βλέπε υποσημείωση 221).

([242]) Μνημόνιο συμφωνίας μεταξύ ICO και UKIC, βλέπε υποσημείωση 231.

([243]) Σε επτά από αυτές τις περιπτώσεις, το ICO συμβούλευσε τον καταγγέλλοντα να αναφέρει το ζήτημα στον υπεύθυνο επεξεργασίας δεδομένων (πρόκειται για την περίπτωση στην οποία ένα πρόσωπο έχει αναφέρει το ζήτημα στο ICO, αλλά θα έπρεπε πρώτα να είχε απευθυνθεί στον υπεύθυνο επεξεργασίας δεδομένων), σε μία από τις περιπτώσεις αυτές, το ICO παρείχε γενικές συμβουλές στον υπεύθυνο επεξεργασίας δεδομένων (αυτό εφαρμόζεται όταν οι ενέργειες του υπευθύνου επεξεργασίας δεν φαίνεται να έχουν γίνει κατά παράβαση της νομοθεσίας, αλλά με τη βελτίωση των πρακτικών θα μπορούσε να είχε αποφευχθεί το ζήτημα που αναφέρθηκε στο ICO), και στις υπόλοιπες 13 περιπτώσεις, δεν χρειάστηκε να αναληφθεί καμία ενέργεια από τον υπεύθυνο επεξεργασίας δεδομένων (αυτό συμβαίνει στις περιπτώσεις όπου τα ζητήματα που αναφέρει το πρόσωπο εμπίπτουν μεν στον νόμο του 2018 για την προστασία των δεδομένων, καθώς αφορούν την επεξεργασία πληροφοριών προσωπικού χαρακτήρα, πλην όμως βάσει των πληροφοριών που παρέχονται, ο υπεύθυνος επεξεργασίας δεν φαίνεται να έχει παραβεί τη νομοθεσία).

([244]) Όπως εξήγησαν οι αρχές του Ηνωμένου Βασιλείου, ο νόμος για τη δικαιοσύνη και την ασφάλεια διεύρυνε το πεδίο αρμοδιοτήτων της ISC, ώστε να συμπεριληφθεί ο ρόλος της εποπτείας της Κοινότητας Πληροφοριών πέραν των τριών υπηρεσιών και να επιτραπεί η αναδρομική εποπτεία των επιχειρησιακών δραστηριοτήτων των υπηρεσιών σε θέματα σημαντικού εθνικού ενδιαφέροντος.

([245]) Άρθρο 1 του JSA 2013. Οι υπουργοί δεν μπορούν να διοριστούν μέλη της επιτροπής. Η θητεία των μελών της ISC διαρκεί όσο και η θητεία του Κοινοβουλίου κατά τη διάρκεια της οποίας διορίστηκαν. Μπορούν να παυθούν από τα καθήκοντά τους με ψήφισμα του σώματος του Κοινοβουλίου από το οποίο διορίστηκαν ή εάν παύσουν να είναι βουλευτές ή αν γίνουν υπουργοί. Τα μέλη μπορούν επίσης να παραιτηθούν.

([246]) Οι εκθέσεις και οι δηλώσεις της ISC διατίθενται ηλεκτρονικά στον ακόλουθο σύνδεσμο: http://isc.independent.gov.uk/committee-reports. Το 2015 η ISC εξέδωσε έκθεση με τίτλο «Privacy and Security: A modern and transparent legal framework» (βλέπε: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf) στην οποία εξετάστηκε το νομικό πλαίσιο για τις τεχνικές παρακολούθησης που χρησιμοποιούν οι υπηρεσίες πληροφοριών και εξέδωσε σειρά συστάσεων οι οποίες στη συνέχεια εξετάστηκαν και ενσωματώθηκαν στο νομοσχέδιο για τις ερευνητικές εξουσίες το οποίο μετατράπηκε σε νόμο, τον νόμο του 2016 για τις ερευνητικές εξουσίες (IPA 2016). Η απάντηση της κυβέρνησης στην έκθεση σχετικά με την προστασία της ιδιωτικότητας και την ασφάλεια διατίθεται στον ακόλουθο σύνδεσμο: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf.

εξέλιξη ([247]). Το μνημόνιο συμφωνίας το οποίο υπογράφηκε μεταξύ του πρωθυπουργού και της ISC ([248]) προσδιορίζει λεπτομερώς τα στοιχεία που πρέπει να λαμβάνονται υπόψη όταν εξετάζεται αν μια δραστηριότητα δεν αποτελεί μέρος μιας επιχείρησης που βρίσκεται σε εξέλιξη ([249]). Ο πρωθυπουργός μπορεί επίσης να ζητήσει από την ISC να διερευνήσει επιχειρήσεις που βρίσκονται σε εξέλιξη και να εξετάσει πληροφορίες που παρέχονται οικειοθελώς από τις υπηρεσίες.

(145) Σύμφωνα με το παράρτημα 1 του JSA 2013, η Επιτροπή Πληροφοριών και Ασφάλειας μπορεί να ζητήσει από τους επικεφαλής οποιασδήποτε από τις τρεις υπηρεσίες πληροφοριών να αποκαλύψουν οποιαδήποτε πληροφορία. Η υπηρεσία πρέπει να παράσχει τις πληροφορίες αυτές, εκτός αν ο υπουργός ασκήσει το δικαίωμα αρνησικυρίας ([250]). Οι αρχές του Ηνωμένου Βασιλείου εξήγησαν ότι στην πράξη είναι ελάχιστες οι πληροφορίες που δεν παρέχονται στην ISC ([251]).

(146) Όσον αφορά τα μέσα προσφυγής, καταρχάς, σύμφωνα με το άρθρο 165 παράγραφος 2 του DPA 2018, το υποκείμενο των δεδομένων μπορεί να υποβάλει καταγγελία στο ICO εάν πιστεύει ότι, σε σχέση με δεδομένα προσωπικού χαρακτήρα που το αφορούν, υφίσταται παράβαση του μέρους 4 του DPA 2018, συμπεριλαμβανομένης τυχόν καταχρηστικής χρήσης των παρεκκλίσεων και περιορισμών εθνικής ασφάλειας.

(147) Επιπλέον, σύμφωνα με το μέρος 4 του DPA 2018, κάθε πρόσωπο έχει το δικαίωμα να υποβάλει αίτηση στο Ανώτερο Δικαστήριο (High Court ή Court of Session στη Σκωτία) για την έκδοση διαταγής με την οποία ζητείται από τον υπεύθυνο επεξεργασίας να συμμορφωθεί με τα δικαιώματα πρόσβασης στα δεδομένα ([252]), αντίταξης στην επεξεργασία ([253]) και διόρθωσης ή διαγραφής.

(148) Τα φυσικά πρόσωπα δικαιούνται επίσης να ζητήσουν αποζημίωση για τη ζημία που υπέστησαν λόγω παράβασης απαίτησης του μέρους 4 του DPA 2018 από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία ([254]). Η ζημία περιλαμβάνει τόσο την οικονομική ζημία όσο και τη μη οικονομική ζημία, όπως την πρόκληση οδύνης ([255]).

(149) Τέλος, ένα φυσικό πρόσωπο μπορεί να υποβάλει καταγγελία στο Ειδικό Δικαιοδοτικό Όργανο Ελέγχου των Ερευνητικών Εξουσιών (Investigatory Powers Tribunal, IPT) για οποιαδήποτε συμπεριφορά εκ μέρους ή για λογαριασμό των υπηρεσιών πληροφοριών του Ηνωμένου Βασιλείου ([256]). Το Ειδικό Δικαιοδοτικό Όργανο Ελέγχου των Ερευνητικών Εξουσιών (IPT) ιδρύθηκε με τον νόμο του 2000 για τη ρύθμιση των ερευνητικών εξουσιών για την Αγγλία, την Ουαλία και τη Βόρεια Ιρλανδία και τον νόμο του 2000 για τη ρύθμιση των ερευνητικών εξουσιών (Σκωτία) για τη Σκωτία (RIPA 2000) και είναι ανεξάρτητο από την εκτελεστική εξουσία ([257]). Σύμφωνα με το άρθρο 65 του RIPA 2000, τα μέλη του IPT διορίζονται από την Αυτής Μεγαλειότητα για πενταετή θητεία.

(150) Τα μέλη του IPT μπορούν να παυθούν από τα καθήκοντά τους από την Αυτής Μεγαλειότητα κατόπιν αναγγελίας ([258]) αμφότερων των σωμάτων του Κοινοβουλίου ([259]).

(151) Για την άσκηση προσφυγής ενώπιον του IPT («απαίτηση ενεργητικής νομιμοποίησης»), σύμφωνα με το άρθρο 65 του RIPA 2000, το πρόσωπο πρέπει να έχει την πεποίθηση i) ότι η συμπεριφορά της υπηρεσίας πληροφοριών έλαβε χώρα σε σχέση με το εν λόγω πρόσωπο, με οποιοδήποτε περιουσιακό του στοιχείο, με οποιαδήποτε επικοινωνία που εστάλη από ή προς το εν λόγω πρόσωπο ή προοριζόταν γι' αυτό, ή με τη χρήση οποιασδήποτε ταχυδρομικής υπηρεσίας, τηλεπικοινωνιακής υπηρεσίας ή συστήματος τηλεπικοινωνιών ([260]), και ii) ότι η συμπεριφορά έλαβε χώρα σε «περιστάσεις δεκτικές

([247]) Άρθρο 2 του JSA 2013.

([248]) Μνημόνιο συμφωνίας μεταξύ του πρωθυπουργού και της ISC, διαθέσιμο στον ακόλουθο σύνδεσμο: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf

([249]) Μνημόνιο συμφωνίας μεταξύ του πρωθυπουργού και της ISC, παράγραφος 14, βλέπε υποσημείωση 248.

([250]) Ο ανώτερος υπουργός μπορεί να ασκήσει δικαίωμα αρνησικυρίας έναντι της κοινολόγησης πληροφοριών μόνο για δύο λόγους: οι πληροφορίες είναι ευαίσθητες και δεν θα πρέπει να κοινολογηθούν στην ISC για λόγους εθνικής ασφάλειας· ή ο χαρακτήρας των πληροφοριών είναι τέτοιος που, σε περίπτωση που υποβαλλόταν αίτημα στον υπουργό να τις προσκομίσει ενώπιον ειδικής επιτροπής ελέγχου των εργασιών των υπουργείων (Departmental Select Committee) της Βουλής των Κοινοτήτων, ο υπουργός θα θεωρούσε ορθό να μην τις προσκομίσει (για λόγους που δεν περιορίζονται στην εθνική ασφάλεια) [Παράρτημα 1 παράγραφος 4 σημείο 2) του JSA 2013].

([251]) UK Explanatory Framework – section H: National Security, σ. 43.

([252]) Άρθρο 94 παράγραφος 11 του DPA 2018.

([253]) Άρθρο 99 παράγραφος 4 του DPA 2018.

([254]) Άρθρο 169 του DPA 2018, το οποίο επιτρέπει την άσκηση αξιώσεων από «πρόσωπο που υφίσταται ζημία λόγω παράβασης απαίτησης της νομοθεσίας για την προστασία των δεδομένων».

([255]) Άρθρο 169 παράγραφος 5 του DPA 2018.

([256]) Βλέπε άρθρο 65 παράγραφος 2 στοιχείο b) του RIPA.

([257]) Σύμφωνα με το παράρτημα 3 του RIPA 2000, τα μέλη πρέπει να διαθέτουν ειδική δικαστική πείρα και η θητεία τους μπορεί να ανανεωθεί.

([258]) Σχετικά με την έννοια της «αναγγελίας», βλέπε υποσημείωση 183.

([259]) Παράρτημα 3 παράγραφος 1 σημείο 5) του RIPA 2000.

([260]) Άρθρο 65 παράγραφος 4 του RIPA 2000.

προσφυγής» ([261]) ή «ασκήθηκε από ή για λογαριασμό των υπηρεσιών πληροφοριών ([262])». Δεδομένου ότι, ειδικότερα, αυτό το κριτήριο της «πεποίθησης» έχει ερμηνευθεί αρκετά ευρέως ([263]), η άσκηση προσφυγής ενώπιον του IPT υπόκειται σε σχετικά χαμηλές απαιτήσεις όσον αφορά την ενεργητική νομιμοποίηση.

(152) Όταν το IPT εξετάζει καταγγελία που έχει υποβληθεί ενώπιόν του, έχει καθήκον να διερευνήσει αν τα πρόσωπα κατά των οποίων προβάλλεται οποιοσδήποτε ισχυρισμός στο πλαίσιο της καταγγελίας έχουν εμπλακεί σε συμπεριφορά που αφορά τον καταγγέλλοντα, καθώς και να ερευνήσει την αρχή η οποία φέρεται να έχει εμπλακεί στις παραβάσεις και αν η προβαλλόμενη συμπεριφορά έλαβε χώρα ([264]). Όταν το IPT επιλαμβάνεται μιας υπόθεσης, οφείλει να εφαρμόζει στη διαδικασία τις ίδιες αρχές με εκείνες που θα εφαρμόζονταν από δικαστήριο επί αίτησης δικαστικού ελέγχου ([265]).

(153) Το IPT πρέπει να ενημερώνει τον καταγγέλλοντα αν έχει εκδοθεί απόφαση υπέρ του ή όχι ([266]). Σύμφωνα με το άρθρο 67 παράγραφοι 6 και 7 του RIPA 2000, το IPT έχει την εξουσία να διατάσσει προσωρινά μέτρα και να επιδικάζει οποιαδήποτε αποζημίωση ή να εκδίδει οποιαδήποτε άλλη απόφαση κρίνει κατάλληλη ([267]). Σύμφωνα με το άρθρο 67A του RIPA 2000, είναι δυνατή η άσκηση προσφυγής κατά απόφασης του IPT, με την επιφύλαξη άδειας που χορηγείται από το εν λόγω όργανο ή το αρμόδιο εφετείο.

(154) Ειδικότερα, τα φυσικά πρόσωπα μπορούν να ασκήσουν αγωγή —και να επιτύχουν επανόρθωση— ενώπιον του IPT σε περίπτωση που θεωρούν ότι μια δημόσια αρχή έχει ενεργήσει (ή προτίθεται να ενεργήσει) κατά τρόπο ασυμβίβαστο με τα δικαιώματα δυνάμει της ΕΣΔΑ, συμπεριλαμβανομένου του δικαιώματος στην προστασία της ιδιωτικής ζωής και των δεδομένων και, ως εκ τούτου, παράνομο βάσει του άρθρου 6 παράγραφος 1 του νόμου του 1998 για τα ανθρώπινα δικαιώματα. Στο IPT έχει απονεμηθεί αποκλειστική αρμοδιότητα για όλες τις αξιώσεις βάσει του νόμου για τα ανθρώπινα δικαιώματα σε σχέση με τις υπηρεσίες πληροφοριών. Αυτό σημαίνει ότι, όπως επισήμανε το Ανώτερο Δικαστήριο, «το αν υπήρξε παράβαση του νόμου για τα ανθρώπινα δικαιώματα βάσει των πραγματικών περιστατικών μιας συγκεκριμένης υπόθεσης είναι κάτι που μπορεί καταρχήν να προβληθεί και να κριθεί από ανεξάρτητο δικαστήριο, το οποίο μπορεί να έχει πρόσβαση σε όλο το σχετικό υλικό, συμπεριλαμβανομένου του απόρρητου υλικού. […] Στο πλαίσιο αυτό, έχουμε επίσης κατά νου ότι υπάρχει πλέον η δυνατότητα προσφυγής κατά του ίδιου του IPT ενώπιον του αρμόδιου εφετείου (για την Αγγλία και την Ουαλία, αυτό είναι το Court of Appeal)· και ότι το Ανώτατο Δικαστήριο αποφάνθηκε πρόσφατα ότι το IPT υπόκειται καταρχήν σε δικαστικό έλεγχο: βλέπε R (Privacy International) κατά Investigatory Powers Tribunal [2019] UKSC 22· [2019] 2 WLR 1219» ([268]). Εάν το IPT διαπιστώσει ότι οποιαδήποτε πράξη δημόσιας αρχής είναι παράνομη, μπορεί να χορηγήσει τη σχετική επανόρθωση ή αποκατάσταση, ή να εκδώσει διαταγή, στο πλαίσιο των αρμοδιοτήτων του όπως κρίνει δίκαιο και κατάλληλο ([269]).

([261]) Οι περιστάσεις αυτές αναφέρονται σε συμπεριφορά δημόσιων αρχών που λαμβάνει χώρα κατόπιν εξουσιοδότησης (π.χ. ένταλμα, άδεια/ειδοποίηση για την απόκτηση δεδομένων επικοινωνιών κ.λπ.), ή εάν οι περιστάσεις είναι τέτοιες ώστε (ανεξάρτητα από το αν υπάρχει ή όχι τέτοια εξουσιοδότηση) δεν θα ήταν ενδεδειγμένο η συμπεριφορά να λάβει χώρα χωρίς αυτή την εξουσιοδότηση, ή τουλάχιστον χωρίς να έχει εξεταστεί δεόντως αν θα έπρεπε να ζητηθεί η εν λόγω εξουσιοδότηση. Συμπεριφορές που έχουν εγκριθεί από δικαστικό επίτροπο (Judicial Commissioner) θεωρείται ότι έλαβαν χώρα υπό περιστάσεις δεκτικές προσφυγής (άρθρο 65 παράγραφος 7ZA του RIPA 2000), ενώ άλλες συμπεριφορές που λαμβάνουν χώρα με την άδεια προσώπου που κατέχει δικαστικό αξίωμα θεωρείται ότι δεν έλαβαν χώρα υπό περιστάσεις δεκτικές προσφυγής (άρθρο 65 παράγραφοι 7 και 8 του RIPA 2000).

([262]) Σύμφωνα με τις πληροφορίες που παρασχέθηκαν από τις αρχές του Ηνωμένου Βασιλείου, το χαμηλό όριο όσον αφορά την ελάχιστη προϋπόθεση για την υποβολή καταγγελίας έχει ως αποτέλεσμα να μην είναι ασυνήθεις οι περιπτώσεις στις οποίες το IPT διαπιστώνει, στο πλαίσιο της διερεύνησης της υπόθεσης, ότι στην πραγματικότητα ο καταγγέλλων ουδέποτε υποβλήθηκε σε έρευνα από δημόσια αρχή. Στην πλέον πρόσφατη στατιστική έκθεση του IPT αναφέρεται ότι το 2016 υποβλήθηκαν στο IPT 209 καταγγελίες, από τις οποίες το 52 % θεωρήθηκαν αβάσιμες ή κακόβουλες, ενώ για το 25 % κρίθηκε ότι δεν ήταν δυνατή η έκδοση απόφασης. Οι αρχές του Ηνωμένου Βασιλείου εξήγησαν ότι αυτό σημαίνει είτε ότι δεν έγινε χρήση μυστικής δραστηριότητας/εξουσίας σε σχέση με τον καταγγέλλοντα είτε ότι έγινε χρήση μυστικών τεχνικών και το IPT έκρινε ότι η δραστηριότητα ήταν νόμιμη. Επιπλέον, το 11 % κρίθηκαν ότι είχαν ασκηθεί αναρμοδίως, αποσύρθηκαν ή δεν ήταν έγκυρες, το 5 % κρίθηκαν εκπρόθεσμες, ενώ για το 7 % των καταγγελιών εκδόθηκε απόφαση υπέρ του καταγγέλλοντος. Statistical Report of the Investigatory Powers Tribunal 2016, διατίθεται στον ακόλουθο σύνδεσμο: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([263]) Βλέπε υπόθεση Human Rights Watch κατά Secretary of State [2016] UKIPTrib15_165-CH. Σ' αυτή την υπόθεση, το IPT, παραπέμποντας στη νομολογία του ΕΔΔΑ, έκρινε ότι το κατάλληλο κριτήριο είναι —όσον αφορά την πεποίθηση ότι οποιαδήποτε συμπεριφορά που εμπίπτει στο άρθρο 68 παράγραφος 5 του RIPA 2000 ασκήθηκε από ή για λογαριασμό οποιασδήποτε από τις υπηρεσίες πληροφοριών— αν υπάρχει οποιοδήποτε έρεισμα για την πεποίθηση αυτή, συμπεριλαμβανομένου του γεγονότος ότι ένα πρόσωπο μπορεί να ισχυριστεί ότι υπήρξε θύμα παραβίασης που προκλήθηκε από την ύπαρξη και μόνο μυστικών μέτρων ή νομοθεσίας που επιτρέπει τη λήψη μυστικών μέτρων, μόνον εφόσον είναι σε θέση να αποδείξει ότι, λόγω της προσωπικής του κατάστασης, διατρέχει ενδεχομένως τον κίνδυνο να υποβληθεί σ' αυτά τα μέτρα (βλέπε Human Rights Watch κατά Secretary of State, σκέψη 41).

([264]) Άρθρο 67 παράγραφος 3 του RIPA 2000.

([265]) Άρθρο 67 παράγραφος 2 του RIPA 2000.

([266]) Άρθρο 68 παράγραφος 4 του RIPA 2000.

([267]) Αυτό μπορεί να περιλαμβάνει διαταγή για την καταστροφή τυχόν αρχείων πληροφοριών που τηρούνται από οποιαδήποτε δημόσια αρχή σε σχέση με οποιοδήποτε πρόσωπο.

([268]) High Court of Justice, Liberty, [2019] EWHC 2057 (Admin), σκέψη 170.

([269]) Άρθρο 8 παράγραφος 1 του νόμου του 1998 για τα ανθρώπινα δικαιώματα.

(155) Αφού εξαντλήσει τα εθνικά ένδικα μέσα, ένα πρόσωπο μπορεί να προσφύγει ενώπιον του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου για παραβιάσεις των δικαιωμάτων που κατοχυρώνονται στην ΕΣΔΑ, συμπεριλαμβανομένου του δικαιώματος στην προστασία της ιδιωτικής ζωής και των δεδομένων.

(156) Από τα ανωτέρω συνάγεται ότι η κοινοποίηση δεδομένων που διαβιβάζονται δυνάμει της παρούσας απόφασης από τις αρχές επιβολής του ποινικού δικαίου του Ηνωμένου Βασιλείου σε άλλες δημόσιες αρχές, συμπεριλαμβανομένων των υπηρεσιών πληροφοριών, πλαισιώνεται από περιορισμούς και όρους που διασφαλίζουν ότι η εν λόγω περαιτέρω κοινοποίηση θα είναι αναγκαία και αναλογική και θα υπόκειται σε ειδικές εγγυήσεις προστασίας των δεδομένων δυνάμει του DPA 2018. Επιπλέον, η επεξεργασία δεδομένων από τις οικείες δημόσιες αρχές εποπτεύεται από ανεξάρτητους φορείς και τα θιγόμενα πρόσωπα έχουν πρόσβαση σε αποτελεσματικά ένδικα μέσα.

3. **ΣΥΜΠΕΡΑΣΜΑ**

(157) Η Επιτροπή θεωρεί ότι το μέρος 3 του DPA 2018 εξασφαλίζει επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται για σκοπούς επιβολής του ποινικού δικαίου από αρμόδιες αρχές της Ένωσης σε αρμόδιες αρχές του Ηνωμένου Βασιλείου, το οποίο είναι κατ' ουσίαν ισοδύναμο με εκείνο που εγγυάται η οδηγία (ΕΕ) 2016/680.

(158) Επιπλέον, η Επιτροπή θεωρεί ότι, συνολικά, οι εποπτικοί μηχανισμοί και τα μέσα προσφυγής που προβλέπονται στη νομοθεσία του Ηνωμένου Βασιλείου επιτρέπουν τον εντοπισμό και την πραγματική τιμωρία των παραβάσεων και προσφέρουν μέσα ένδικης προστασίας στα υποκείμενα των δεδομένων προκειμένου να επιτυγχάνουν την πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που τα αφορούν και, τελικώς, τη διόρθωση ή τη διαγραφή των εν λόγω δεδομένων.

(159) Τέλος, βάσει των διαθέσιμων πληροφοριών σχετικά με την έννομη τάξη του Ηνωμένου Βασιλείου, η Επιτροπή θεωρεί ότι οποιαδήποτε επέμβαση στα θεμελιώδη δικαιώματα των φυσικών προσώπων των οποίων τα δεδομένα προσωπικού χαρακτήρα διαβιβάζονται από την Ευρωπαϊκή Ένωση στο Ηνωμένο Βασίλειο από δημόσιες αρχές του Ηνωμένου Βασιλείου για σκοπούς δημόσιου συμφέροντος, μεταξύ άλλων και στο πλαίσιο της κοινοποίησης δεδομένων προσωπικού χαρακτήρα μεταξύ αρχών επιβολής του νόμου και άλλων δημόσιων αρχών, όπως φορέων εθνικής ασφάλειας, θα περιορίζεται στο απολύτως αναγκαίο για την επίτευξη του εν λόγω νόμιμου σκοπού, και ότι υφίσταται αποτελεσματική νομική προστασία κατά της επέμβασης αυτού του είδους.

(160) Ως εκ τούτου, θα πρέπει να αποφασιστεί ότι το Ηνωμένο Βασίλειο εξασφαλίζει επαρκές επίπεδο προστασίας κατά την έννοια του άρθρου 36 παράγραφος 2 της οδηγίας (ΕΕ) 2016/680, ερμηνευόμενου υπό το πρίσμα του Χάρτη των Θεμελιωδών Δικαιωμάτων.

(161) Το συμπέρασμα αυτό βασίζεται τόσο στο σχετικό εσωτερικό καθεστώς του Ηνωμένου Βασιλείου όσο και στις διεθνείς δεσμεύσεις του, ειδικότερα τις δεσμεύσεις για την τήρηση της Ευρωπαϊκής σύμβασης Δικαιωμάτων του Ανθρώπου και την υπαγωγή του στη δικαιοδοσία του Ευρωπαϊκού Δικαστηρίου των Δικαιωμάτων του Ανθρώπου. Ως εκ τούτου, η συνεχής τήρηση των εν λόγω διεθνών υποχρεώσεων αποτελεί ιδιαίτερα σημαντικό στοιχείο της αξιολόγησης στην οποία βασίζεται η παρούσα απόφαση.

4. **ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΗΣ ΠΑΡΟΥΣΑΣ ΑΠΟΦΑΣΗΣ ΚΑΙ ΔΡΑΣΗ ΤΩΝ ΑΡΧΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΩΝ ΔΕΔΟΜΕΝΩΝ**

(162) Τα κράτη μέλη και τα όργανά τους υποχρεούνται να λαμβάνουν τα αναγκαία μέτρα προκειμένου να συμμορφώνονται με τις νομοθετικές πράξεις των θεσμικών οργάνων της Ένωσης, καθώς αυτές θεωρείται ότι είναι σύννομες και, ως εκ τούτου, παράγουν έννομα αποτελέσματα έως ότου λήξουν, ανακληθούν, ακυρωθούν μετά από αγωγή ακύρωσης ή κηρυχθούν άκυρες μετά από υποβολή προδικαστικού ερωτήματος ή άσκηση αγωγής με αιτιολογία τον παράνομο χαρακτήρα.

(163) Κατά συνέπεια, η απόφαση περί επάρκειας που εκδίδεται από την Επιτροπή δυνάμει του άρθρου 36 παράγραφος 3 της οδηγίας (ΕΕ) 2016/680 είναι δεσμευτική για όλα τα όργανα των κρατών μελών στα οποία απευθύνεται η εν λόγω απόφαση, συμπεριλαμβανομένων των ανεξάρτητων εποπτικών αρχών τους. Ιδίως, κατά τη διάρκεια της περιόδου εφαρμογής της παρούσας απόφασης, οι διαβιβάσεις από υπεύθυνο επεξεργασίας ή εκτελούντα την επεξεργασία στην Ευρωπαϊκή Ένωση προς υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία στο Ηνωμένο Βασίλειο μπορούν να πραγματοποιούνται χωρίς να απαιτείται περαιτέρω άδεια.

(164) Ταυτόχρονα, θα πρέπει να υπενθυμιστεί ότι, σύμφωνα με το άρθρο 47 παράγραφος 5 της οδηγίας (ΕΕ) 2016/680, και όπως εξήγησε το Δικαστήριο στην απόφαση Schrems, όταν μια εθνική αρχή προστασίας των δεδομένων αμφισβητεί, μεταξύ άλλων κατόπιν καταγγελίας, τη συμβατότητα μιας απόφασης περί επάρκειας την οποία έχει εκδώσει η Επιτροπή με τα θεμελιώδη δικαιώματα του προσώπου στην προστασία της ιδιωτικής ζωής και των δεδομένων, το εθνικό δίκαιο πρέπει να της παρέχει μέσα ένδικης προστασίας ώστε να μπορεί να προβάλει τις αιτιάσεις αυτές ενώπιον εθνικού δικαστηρίου, το οποίο μπορεί να χρειαστεί να υποβάλει προδικαστικό ερώτημα στο Δικαστήριο ([270]).

([270]) Schrems, σκέψη 65.

5. **ΠΑΡΑΚΟΛΟΥΘΗΣΗ, ΑΝΑΣΤΟΛΗ, ΚΑΤΑΡΓΗΣΗ Ή ΤΡΟΠΟΠΟΙΗΣΗ ΤΗΣ ΠΑΡΟΥΣΑΣ ΑΠΟΦΑΣΗΣ**

(165) Σύμφωνα με το άρθρο 36 παράγραφος 4 της οδηγίας (ΕΕ) 2016/680, η Επιτροπή πρέπει να παρακολουθεί, σε συνεχή βάση, τις σχετικές εξελίξεις στο Ηνωμένο Βασίλειο μετά την έκδοση της παρούσας απόφασης, προκειμένου να αξιολογεί αν εξακολουθεί να διασφαλίζει κατ' ουσίαν ισοδύναμο επίπεδο προστασίας. Η εν λόγω παρακολούθηση είναι ιδιαίτερα σημαντική στην προκειμένη περίπτωση, καθώς το Ηνωμένο Βασίλειο θα διαχειρίζεται, θα εφαρμόζει και θα επιβάλλει ένα νέο καθεστώς προστασίας των δεδομένων το οποίο δεν θα υπόκειται πλέον στο δίκαιο της Ένωσης και το οποίο ενδέχεται να εξελιχθεί. Στο πλαίσιο αυτό, θα δοθεί ιδιαίτερη προσοχή στην εφαρμογή στην πράξη των κανόνων του Ηνωμένου Βασιλείου σχετικά με τις διαβιβάσεις δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες, μεταξύ άλλων μέσω της σύναψης διεθνών συμφωνιών, και στον αντίκτυπο που μπορεί να έχει στο επίπεδο προστασίας που παρέχεται στα δεδομένα που διαβιβάζονται δυνάμει της παρούσας απόφασης· καθώς και για την αποτελεσματικότητα της άσκησης των ατομικών δικαιωμάτων στους τομείς που καλύπτονται από την παρούσα απόφαση. Μεταξύ άλλων στοιχείων, οι εξελίξεις στη νομολογία και η εποπτεία από το ICO και άλλους ανεξάρτητους φορείς θα τροφοδοτούν την παρακολούθηση της Επιτροπής.

(166) Με σκοπό να διευκολυνθεί η παρακολούθηση, οι αρχές του Ηνωμένου Βασιλείου θα πρέπει να ενημερώνουν την Επιτροπή αμέσως και σε τακτική βάση για κάθε ουσιώδη μεταβολή στην έννομη τάξη του Ηνωμένου Βασιλείου που έχει αντίκτυπο στο νομικό πλαίσιο που αποτελεί το αντικείμενο της παρούσας απόφασης, καθώς και για κάθε εξέλιξη των πρακτικών που σχετίζονται με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα οι οποίες αξιολογούνται στην παρούσα απόφαση, ιδίως αναφορικά με τα στοιχεία που αναφέρονται στην αιτιολογική σκέψη (165).

(167) Επιπροσθέτως, για να μπορεί η Επιτροπή να εκτελέσει με αποτελεσματικότητα το καθήκον της παρακολούθησης, τα κράτη μέλη θα πρέπει να ενημερώνουν την Επιτροπή για κάθε συναφή δράση των εθνικών αρχών προστασίας δεδομένων, ιδίως σε σχέση με ερωτήσεις ή καταγγελίες από υποκείμενα δεδομένων της ΕΕ σχετικά με τη διαβίβαση δεδομένων προσωπικού χαρακτήρα από την Ένωση σε αρμόδιες αρχές στο Ηνωμένο Βασίλειο. Η Επιτροπή θα πρέπει επίσης να λαμβάνει γνώση οποιασδήποτε ένδειξης ότι οι ενέργειες των δημόσιων αρχών του Ηνωμένου Βασιλείου που είναι αρμόδιες για την πρόληψη, τη διερεύνηση, την ανίχνευση ή τη δίωξη ποινικών αδικημάτων, συμπεριλαμβανομένων των εποπτικών φορέων, δεν διασφαλίζουν το απαιτούμενο επίπεδο προστασίας.

(168) Σε περίπτωση που οι διαθέσιμες πληροφορίες, ειδικότερα οι πληροφορίες που προκύπτουν από την παρακολούθηση της παρούσας απόφασης ή που παρέχονται από τις αρχές του Ηνωμένου Βασιλείου ή των κρατών μελών, αποκαλύπτουν ότι το επίπεδο προστασίας που παρέχει το Ηνωμένο Βασίλειο ενδέχεται να μην είναι πλέον επαρκές, η Επιτροπή θα πρέπει να ενημερώσει σχετικά τις αρμόδιες αρχές του Ηνωμένου Βασιλείου και να ζητήσει τη λήψη κατάλληλων μέτρων εντός καθορισμένου χρονικού διαστήματος που δεν επιτρέπεται να υπερβαίνει τους τρεις μήνες. Εφόσον είναι αναγκαίο, η περίοδος αυτή μπορεί να παραταθεί για συγκεκριμένο χρονικό διάστημα, λαμβανομένης υπόψη της φύσης του επίμαχου ζητήματος και/ή των μέτρων που πρέπει να ληφθούν.

(169) Εάν, κατά τη λήξη της εν λόγω καθορισμένης προθεσμίας, οι αρμόδιες αρχές του Ηνωμένου Βασιλείου δεν λάβουν τα εν λόγω μέτρα ή δεν αποδείξουν με άλλον τρόπο ικανοποιητικά ότι η παρούσα απόφαση εξακολουθεί να βασίζεται σε επαρκές επίπεδο προστασίας, η Επιτροπή θα κινήσει τη διαδικασία που αναφέρεται στο άρθρο 58 παράγραφος 2 της οδηγίας (ΕΕ) 2016/680 με σκοπό τη μερική ή πλήρη αναστολή ή κατάργηση της παρούσας απόφασης.

(170) Εναλλακτικά, η Επιτροπή θα κινήσει την εν λόγω διαδικασία για την τροποποίηση της απόφασης, ιδίως με την υποβολή των διαβιβάσεων δεδομένων σε πρόσθετες προϋποθέσεις ή τον περιορισμό του πεδίου εφαρμογής της διαπίστωσης επάρκειας μόνο στις διαβιβάσεις δεδομένων για τις οποίες εξακολουθεί να διασφαλίζεται επαρκές επίπεδο προστασίας.

(171) Όταν συντρέχουν δεόντως αιτιολογημένοι επιτακτικοί λόγοι επείγουσας ανάγκης, η Επιτροπή θα κάνει χρήση της δυνατότητας να εκδώσει, σύμφωνα με τη διαδικασία που αναφέρεται στο άρθρο 58 παράγραφος 3 της οδηγίας (ΕΕ) 2016/680, εκτελεστικές πράξεις άμεσης εφαρμογής για την αναστολή, την κατάργηση ή την τροποποίηση της απόφασης.

6. **ΔΙΑΡΚΕΙΑ ΚΑΙ ΑΝΑΝΕΩΣΗ ΤΗΣ ΠΑΡΟΥΣΑΣ ΑΠΟΦΑΣΗΣ**

(172) Θα πρέπει να ληφθεί υπόψη ότι, με τη λήξη της μεταβατικής περιόδου που προβλέπεται από τη συμφωνία αποχώρησης και μόλις παύσει να ισχύει η μεταβατική διάταξη του άρθρου 782 της συμφωνίας εμπορίου και συνεργασίας ΕΕ–Ηνωμένου Βασιλείου, το Ηνωμένο Βασίλειο θα διαχειρίζεται, θα εφαρμόζει και θα επιβάλλει ένα νέο καθεστώς προστασίας δεδομένων αντί εκείνου που ίσχυε όταν δεσμευόταν από το δίκαιο της Ευρωπαϊκής Ένωσης. Αυτό μπορεί να περιλαμβάνει κυρίως τροποποιήσεις ή αλλαγές στο πλαίσιο προστασίας δεδομένων το οποίο αξιολογείται στην παρούσα απόφαση, καθώς και άλλες σχετικές εξελίξεις.

(173) Ως εκ τούτου, είναι σκόπιμο να προβλεφθεί ότι η παρούσα απόφαση θα εφαρμόζεται για περίοδο τεσσάρων ετών από την έναρξη ισχύος της.

(174) Σε περίπτωση, ιδίως, που οι πληροφορίες που προκύπτουν από την παρακολούθηση της παρούσας απόφασης αποκαλύψουν ότι οι διαπιστώσεις σχετικά με την επάρκεια του επιπέδου προστασίας που εξασφαλίζεται στο Ηνωμένο Βασίλειο εξακολουθούν να είναι αντικειμενικά και νομικά αιτιολογημένες, η Επιτροπή θα πρέπει, το αργότερο έξι μήνες πριν από τη λήξη ισχύος της παρούσας απόφασης, να κινήσει τη διαδικασία τροποποίησης της παρούσας απόφασης επεκτείνοντας, καταρχήν, το χρονικό πεδίο εφαρμογής της για πρόσθετη περίοδο τεσσάρων ετών. Κάθε τέτοια εκτελεστική πράξη που τροποποιεί την παρούσα απόφαση πρέπει να εκδίδεται σύμφωνα με τη διαδικασία που αναφέρεται στο άρθρο 58 παράγραφος 2 της οδηγίας (ΕΕ) 2016/680.

7. **ΤΕΛΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ**

(175) Το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων δημοσίευσε τη γνώμη του ([271]), η οποία ελήφθη υπόψη κατά την εκπόνηση της παρούσας απόφασης.

(176) Τα μέτρα που προβλέπονται στην παρούσα απόφαση είναι σύμφωνα με τη γνώμη της επιτροπής που έχει συσταθεί βάσει του άρθρου 58 της οδηγίας (ΕΕ) 2016/680.

(177) Σύμφωνα με το άρθρο 6α του πρωτοκόλλου αριθ. 21 για τη θέση του Ηνωμένου Βασιλείου και της Ιρλανδίας όσον αφορά τον χώρο ελευθερίας, ασφάλειας και δικαιοσύνης, το οποίο προσαρτάται στη ΣΕΕ και στη ΣΛΕΕ, η Ιρλανδία δεν δεσμεύεται από τους κανόνες που θεσπίζονται στην οδηγία (ΕΕ) 2016/680 και, ως εκ τούτου, από την παρούσα εκτελεστική απόφαση, σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του τρίτου μέρους τίτλος V κεφάλαια 4 ή 5 της ΣΛΕΕ, εφόσον η Ιρλανδία δεν δεσμεύεται από τους κανόνες οι οποίοι διέπουν μορφές δικαστικής συνεργασίας σε ποινικές υποθέσεις ή αστυνομικής συνεργασίας στο πλαίσιο των οποίων πρέπει να τηρούνται οι διατάξεις οι οποίες θεσπίζονται βάσει του άρθρου 16 της ΣΛΕΕ. Επιπλέον, δυνάμει της εκτελεστικής απόφασης (ΕΕ) 2020/1745 του Συμβουλίου ([272]), η οδηγία (ΕΕ) 2016/680 θα τεθεί σε ισχύ και θα εφαρμόζεται σε προσωρινή βάση στην Ιρλανδία από την 1η Ιανουαρίου 2021. Ως εκ τούτου, η Ιρλανδία δεσμεύεται από την παρούσα εκτελεστική απόφαση, υπό τις ίδιες προϋποθέσεις που ισχύουν για την εφαρμογή της οδηγίας (ΕΕ) 2016/680 στην Ιρλανδία, όπως ορίζεται στην εκτελεστική απόφαση (ΕΕ) 2020/1745 όσον αφορά το κεκτημένο του Σένγκεν στο οποίο συμμετέχει.

(178) Σύμφωνα με τα άρθρα 2 και 2α του πρωτοκόλλου αριθ. 22 σχετικά με τη θέση της Δανίας, το οποίο προσαρτάται στη Συνθήκη για την Ευρωπαϊκή Ένωση και στη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης, η Δανία δεν δεσμεύεται από τους κανόνες που θεσπίζονται στην οδηγία (ΕΕ) 2016/680 και, ως εκ τούτου, από την παρούσα εκτελεστική απόφαση, ούτε υπόκειται στην εφαρμογή τους σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τα κράτη μέλη κατά την άσκηση δραστηριοτήτων που εμπίπτουν στο πεδίο εφαρμογής του τρίτου μέρους τίτλος V κεφάλαια 4 ή 5 της ΣΛΕΕ. Ωστόσο, επειδή η οδηγία (ΕΕ) 2016/680 βασίζεται στο κεκτημένο του Σένγκεν, η Δανία κοινοποίησε στις 26 Οκτωβρίου 2016, σύμφωνα με το άρθρο 4 του εν λόγω πρωτοκόλλου, την απόφασή της να εφαρμόζει την οδηγία (ΕΕ) 2016/680. Ως εκ τούτου, η Δανία δεσμεύεται, βάσει του διεθνούς δικαίου, να εφαρμόζει την παρούσα εκτελεστική απόφαση.

(179) Όσον αφορά την Ισλανδία και τη Νορβηγία, η παρούσα εκτελεστική απόφαση συνιστά ανάπτυξη των διατάξεων του κεκτημένου του Σένγκεν, όπως προβλέπεται από τη συμφωνία που έχει συναφθεί από το Συμβούλιο της Ευρωπαϊκής Ένωσης και από τη Δημοκρατία της Ισλανδίας και το Βασίλειο της Νορβηγίας σχετικά με τη σύνδεση των δύο αυτών κρατών προς τη θέση σε ισχύ, την εφαρμογή και την ανάπτυξη του κεκτημένου του Σένγκεν ([273]).

(180) Όσον αφορά την Ελβετία, η παρούσα εκτελεστική απόφαση συνιστά ανάπτυξη των διατάξεων του κεκτημένου του Σένγκεν όπως προβλέπεται από τη συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης, της Ευρωπαϊκής Κοινότητας και της Ελβετικής Συνομοσπονδίας σχετικά με τη σύνδεση της Ελβετικής Συνομοσπονδίας προς τη θέση σε ισχύ, την εφαρμογή και την ανάπτυξη του κεκτημένου του Σένγκεν ([274]).

(181) Όσον αφορά το Λιχτενστάιν, η παρούσα εκτελεστική απόφαση αποτελεί ανάπτυξη των διατάξεων του κεκτημένου του Σένγκεν, όπως προβλέπεται από το πρωτόκολλο μεταξύ της Ευρωπαϊκής Ένωσης, της Ευρωπαϊκής Κοινότητας, της Ελβετικής Συνομοσπονδίας και του Πριγκιπάτου του Λιχτενστάιν για την προσχώρηση του Πριγκιπάτου του Λιχτενστάιν στη συμφωνία μεταξύ της Ευρωπαϊκής Ένωσης, της Ευρωπαϊκής Κοινότητας και της Ελβετικής Συνομοσπονδίας σχετικά με τη σύνδεση της Ελβετικής Συνομοσπονδίας προς τη θέση σε ισχύ, την εφαρμογή και την ανάπτυξη του κεκτημένου του Σένγκεν ([275]),

---

([271]) Γνώμη 15/2021 σχετικά με το σχέδιο εκτελεστικής απόφασης της Ευρωπαϊκής Επιτροπής σύμφωνα με την οδηγία (ΕΕ) 2016/680 σχετικά με την επάρκεια της προστασίας των δεδομένων προσωπικού χαρακτήρα στο Ηνωμένο Βασίλειο, διατίθεται στον ακόλουθο σύνδεσμο: https://edpb.europa.eu/our-work-tools/our-documents/opinion-led/opinion-152021-regarding-european-commission-draft_el.

([272]) Εκτελεστική απόφαση (ΕΕ) 2020/1745 του Συμβουλίου, της 18ης Νοεμβρίου 2020, σχετικά με τη θέση σε ισχύ των διατάξεων του κεκτημένου Σένγκεν όσον αφορά την προστασία των δεδομένων και σχετικά με την προσωρινή θέση σε ισχύ ορισμένων διατάξεων του κεκτημένου Σένγκεν στην Ιρλανδία (ΕΕ L 393 της 23.11.2020, σ. 3).

([273]) ΕΕ L 176 της 10.7.1999, σ. 36.

([274]) ΕΕ L 53 της 27.2.2008, σ. 52.

([275]) ΕΕ L 160 της 18.6.2011, σ. 21.

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Για τους σκοπούς του άρθρου 36 της οδηγίας (ΕΕ) 2016/680, το Ηνωμένο Βασίλειο διασφαλίζει επαρκές επίπεδο προστασίας των δεδομένων προσωπικού χαρακτήρα που διαβιβάζονται από την Ευρωπαϊκή Ένωση σε δημόσιες αρχές του Ηνωμένου Βασιλείου που είναι αρμόδιες για την πρόληψη, τη διερεύνηση, την ανίχνευση ή τη δίωξη ποινικών αδικημάτων ή την εκτέλεση ποινικών κυρώσεων.

Άρθρο 2

Όταν οι αρμόδιες εποπτικές αρχές των κρατών μελών, με στόχο την προστασία φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα τους, ασκούν τις εξουσίες τους δυνάμει του άρθρου 47 της οδηγίας (ΕΕ) 2016/680 σε σχέση με διαβιβάσεις δεδομένων σε δημόσιες αρχές του Ηνωμένου Βασιλείου που εμπίπτουν στο πεδίο εφαρμογής που ορίζεται στο άρθρο 1, το οικείο κράτος μέλος ενημερώνει χωρίς καθυστέρηση την Επιτροπή.

Άρθρο 3

1. Η Επιτροπή παρακολουθεί σε συνεχή βάση την εφαρμογή του νομικού πλαισίου στο οποίο βασίζεται η παρούσα απόφαση, συμπεριλαμβανομένων των όρων υπό τους οποίους πραγματοποιούνται οι περαιτέρω διαβιβάσεις και ασκούνται τα ατομικά δικαιώματα, προκειμένου να αξιολογεί αν το Ηνωμένο Βασίλειο εξακολουθεί να διασφαλίζει επαρκές επίπεδο προστασίας κατά την έννοια του άρθρου 1.

2. Τα κράτη μέλη ενημερώνουν την Επιτροπή, και αντιστρόφως, για περιπτώσεις στις οποίες ο Επίτροπος Πληροφοριών ή οποιαδήποτε άλλη αρμόδια αρχή του Ηνωμένου Βασιλείου δεν διασφαλίζει τη συμμόρφωση με το νομικό πλαίσιο στο οποίο βασίζεται η παρούσα απόφαση.

3. Τα κράτη μέλη ενημερώνουν την Επιτροπή, και αντιστρόφως, για κάθε ένδειξη ότι παρεμβάσεις των δημόσιων αρχών του Ηνωμένου Βασιλείου στο δικαίωμα των φυσικών προσώπων για προστασία των δεδομένων τους προσωπικού χαρακτήρα υπερβαίνουν το απολύτως αναγκαίο ή ότι δεν παρέχεται αποτελεσματική έννομη προστασία κατά των εν λόγω επεμβάσεων.

4. Όταν η Επιτροπή έχει ενδείξεις ότι δεν διασφαλίζεται πλέον επαρκές επίπεδο προστασίας, ενημερώνει τις αρμόδιες αρχές του Ηνωμένου Βασιλείου και μπορεί να αναστείλει, να καταργήσει ή να τροποποιήσει την παρούσα απόφαση.

5. Η Επιτροπή μπορεί επίσης να αναστείλει, να καταργήσει ή να τροποποιήσει την παρούσα απόφαση εάν η απροθυμία συνεργασίας της κυβέρνησης του Ηνωμένου Βασιλείου δεν επιτρέπει στην Επιτροπή να προσδιορίσει κατά πόσον επηρεάζεται η διαπίστωση του άρθρου 1.

Άρθρο 4

Η παρούσα απόφαση λήγει στις 27 Ιουνίου 2025, εκτός εάν η ισχύς της παραταθεί σύμφωνα με τη διαδικασία που αναφέρεται στο άρθρο 58 παράγραφος 2 της οδηγίας (ΕΕ) 2016/680.

Άρθρο 5

Η παρούσα απόφαση απευθύνεται στα κράτη μέλη.

Βρυξέλλες, 28 Ιουνίου 2021.

Για την Επιτροπή
Didier REYNDERS
Μέλος της Επιτροπής