ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Ταχ. Δ/νση: ΟΜΗΡΟΥ 8
105 64 ΑΘΗΝΑ
ΤΗΛ.: 33.52.604-605
FAX: 33.52.617

Αθήνα 20/09/2001
Αρ. Πρωτ. 1830

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτικές συνεδρίασεις κατά τις ημερομηνίες 22/01/2001, 12/02/2001, 22/02/2001, 12/03/2001, 09/04/2001, 27/04/2001, 18/06/2001 στο κατάστημά της αποτελούμενη από τον κ. Κ. Δαφέρμο, Πρόεδρο, και τους κ. κ. Α. Παπαχρίστου, Ν. Αλιβιζάτο, Ε. Κιουντούζη, Β. Παπαπετρόπουλο, Σ. Λύτρα, Π. Πάγκαλο, τακτικά μέλη, για να συζητήσει για την έκδοσης Οδηγίας με θέμα τα αρχεία των εργαζομένων. Χρέη εισηγητή στην υπόθεση με εντολή Προέδρου είχε αναλάβει η κ. Ε. Μήτρου. Παρούσα χωρίς δικαίωμα ψήφου ήταν η κ. Ε. Τσιγγάνου, Γραμματέας.

Η κ. Ε. Μήτρου ανέπτυξε προφορικά την από 10/06/2001 εισήγησή της. Επακολούθησε διεξοδική συζήτηση και, σύμφωνα με το άρθρο 19§1 περ. θ΄, ν.2472/1997, η Αρχή εξέδωσε την ακόλουθη οδηγία

Ο Δ Η Γ Ι Α Αρ. 115 / 2001

Α' ΠΡΟΛΕΓΟΜΕΝΑ

Κατά την διάρκεια της θητείας της η Αρχή Προστασίας Προσωπικών Δεδομένων αντιμετώπισε πολλές φορές ζητήματα που αφορούν την προστασία των προσωπικών δεδομένων στο πεδίο των εργασιακών σχέσεων. Ειδικότερα, είτε ύστερα από καταγγελία μεμονωμένων εργαζομένων αλλά και συλλογικών οργανώσεών τους είτε με αφορμή δημοσιεύματα του

τύπου, η Αρχή ασχολήθηκε με ζητήματα που άπτονται της παρακολούθησης επικοινωνιών των εργαζομένων, της επιτήρησης των χώρων εργασίας, της διαβίβασης δεδομένων των εργαζομένων σε τρίτους, της χρήσης βιομετρικών μεθόδων για τον έλεγχο της πρόσβασης στο χώρο εργασίας κ.ά.. και εξέδωσε σειρά αποφάσεων. Ενδεικτικά αναφέρονται η με αριθμό 245/2000 απόφαση με την οποία καθορίζεται η επεξεργασία προσωπικών δεδομένων εργαζομένων για τον έλεγχο εισόδου και εξόδου τους στους χώρους εργασίας με τη μέθοδο της δακτυλοσκόπησης, καθώς και η με αριθμό 637/18/2000 απόφαση που αφορά τον έλεγχο των τηλεφωνημάτων των εργαζομένων στον χώρο εργασίας.

Κατά την εξέταση των σχετικών υποθέσεων η Αρχή διαπίστωσε:
α) την ευρεία έκταση της επεξεργασίας προσωπικών δεδομένων των εργαζομένων και την ένταση της χρήσης μεθόδων παρακολούθησης.
β) την αναγκαιότητα και ταυτόχρονα τη δυσχέρεια εξειδίκευσης της στάθμισης και δικαιωμάτων στο πλαίσιο της εργασιακής σχέσης, η οποία χαρακτηρίζεται κατά κανόνα από μία εγγενή ανισότητα των μερών. Η επεξεργασία δεδομένων επί τη βάσει της συγκατάθεσης ή της εκπλήρωσης υποχρεώσεων από την σύμβαση εργασίας (άρθρα 5 και 7 του Ν. 2472/97 όπως ισχύει) είναι μεν νόμιμη αλλά, όπως διαπιστώνει η Αρχή, η αφηρημένη κανονιστική διατύπωση δεν λαμβάνει υπόψη το στοιχείο της εξάρτησης στο πλαίσιο της σχέσης εργασίας. Το στοιχείο αυτό αποδυναμώνει την βαρύτητα της ελεύθερης συγκατάθεσης ή της ελεύθερης διαμόρφωσης του περιεχομένου της σύμβασης.
γ) την διαθεσιμότητα και χρήση πολλών νέων τεχνικών μεθόδων για την επιτήρηση των εργαζομένων, που θέτουν νέα ζητήματα όπως είναι η έκταση του ελέγχου του ηλεκτρονικού ταχυδρομείου ή η χρήση βιομετρικών μεθόδων για την οργάνωση της εργασίας .

Αξίζει να επισημανθεί ότι ανάλογες διαπιστώσεις και, κυρίως, η επισήμανση της ανεπάρκειας της συγκατάθεσης ως αυτοτελούς βάσης για την επεξεργασία προσωπικών δεδομένων των εργαζομένων διατρέχουν και καθορίζουν το πρόσφατο κείμενο εργασίας της Ευρωπαϊκής Επιτροπής

σχετικά με τα θέματα προστασίας των προσωπικών δεδομένων στο πλαίσιο της απασχόλησης.

Η Αρχή έχει ήδη αντιμετωπίσει τα συγκεκριμένα θέματα που έχουν τεθεί με τους γενικούς κανόνες που έχει εισαγάγει ο νομοθέτης με τους Ν. 2472/97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και Ν. 2774/99 για την προστασία προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα. Ωστόσο διαπιστώνει ότι η εφαρμογή των γενικών κανόνων, λόγω της οριζόντιας φύσης τους, δεν λαμβάνει υπόψη τους ιδιαίτερους σκοπούς, τις συνθήκες και γενικά το περιβάλλον της εργασιακής σχέσης. Αυτό μπορεί να οδηγήσει σε ερμηνευτικά προβλήματα και σε ανασφάλεια δικαίου που ενδέχεται μάλιστα να προβληθούν ως πρόσχημα για την ένταση του ελέγχου των εργαζομένων και τον περιορισμό των δικαιωμάτων τους. Οι σχετικοί προβληματισμοί της Αρχής ενισχύονται από το γεγονός ότι ο Ν. 2819/2000 (άρθρο 8 που προσθέτει νέο άρθρο 7^{A}) επέφερε τροποποιήσεις στον Ν. 2472/97 και - μεταξύ των άλλων- εξαιρεί την επεξεργασία των προσωπικών δεδομένων που πραγματοποιείται στο πεδίο των σχέσεων εργασίας από τις υποχρεώσεις γνωστοποίησης και αίτησης για άδεια. Συνεπώς, ο υπεύθυνος επεξεργασίας που, στις περισσότερες περιπτώσεις (είτε τυπικά είτε κατ΄ αποτέλεσμα) ταυτίζεται με τον εργοδότη ή τον προϊστάμενο, ορίζει κατ΄ αρχήν μόνος του τους όρους της επεξεργασίας προσωπικών δεδομένων – υποκείμενος βέβαια σε κάθε περίπτωση στον κατασταλτικό έλεγχο της Αρχής. Πρέπει να σημειωθεί η νέα πρόσφατη τροποποίηση της σχετικής παραγράφου του άρθρου 7^{A} (άρθρο 34 Ν. 2915/01 ΦΕΚ 109 Α') με την οποία αίρεται κάθε αμφιβολία για την εφαρμογή της προαναφερόμενης ρύθμισης και στον δημόσιο τομέα. Είναι αυτονόητο ότι η παραπάνω διάταξη αφορά τις περιπτώσεις που η συλλογή και επεξεργασία προσωπικών δεδομένων γίνεται αποκλειστικά για την εξυπηρέτηση της σχέσης εργασίας. Επομένως, αν αναφέρεται μόνο έμμεσα σε αυτήν ή αν ο υπεύθυνος επεξεργασίας προβαίνει σε διαβίβαση δεδομένων σε τρίτους δεν απαλλάσσεται από την υποχρέωση γνωστοποίησης ή αίτησης αδείας.

Για τους λόγους αυτούς η Αρχή Προστασίας Δεδομένων, ασκώντας την αρμοδιότητα του άρθρου 19 παρ. 1 α, έκρινε σκόπιμη την έκδοση της

παρούσας Οδηγίας, με την οποία ερμηνεύονται οι κανόνες των Ν. 2472/97 και 2774/99, ώστε να είναι ευκολότερη και σαφέστερη η εφαρμογή των επιταγών του νόμου, με σκοπό την αποτελεσματική προστασία των προσωπικών δεδομένων των εργαζομένων. Η χρησιμότητα της ενιαίας εφαρμογής των θεμάτων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε ειδικούς τομείς, και επομένως και στον τομέα των εργασιακών σχέσεων, είναι αυτονόητη και χρήσιμη. Η ενιαία εφαρμογή της χρήσης των προσωπικών δεδομένων στον τομέα της εργασίας, στο σημαντικότερο βάθρο δηλ. της κοινωνικής συνοχής, θα συντελέσει στην ασφάλεια του δικαίου και στη γνώση των δικαιωμάτων και των υποχρεώσεων των κοινωνικών εταίρων. Στο πλαίσιο αυτό θα πρέπει να τονιστούν τα ακόλουθα:

1. Η Οδηγία αυτή, εκδίδεται με σκοπό να καθορισθούν τα ακραία όρια εντός των οποίων ο εργοδότης/ προϊστάμενος, ασκώντας το διευθυντικό του δικαίωμα και δικαίωμα οργάνωσης της επιχείρησης, δικαιούται, κατά την κείμενη νομοθεσία, να επεξεργάζεται τα προσωπικά δεδομένα των εργαζόμενων.
2. Η Οδηγία δεν θέτει νέους κανόνες δικαίου, πρωτογενείς ή δευτερογενείς. Με αυτήν επιχειρείται ερμηνευτική εξειδίκευση της νομοθεσίας περί προστασίας των προσωπικών δεδομένων κατά την εκτέλεση της εργασιακής σχέσης. Δηλαδή η Αρχή Προστασίας Προσωπικών Δεδομένων, προσπαθώντας να συλλάβει τις περιπτώσεις επεξεργασίας που είναι δυνατό να εμφανισθούν κατά την εκτέλεση της εργασιακής σχέσης και έχοντας υπόψη την κείμενη νομοθεσία, προβαίνει στην κατά την κρίση της ερμηνεία, αφήνοντας έτσι να διαφανεί πώς θα έκρινε στο μέλλον μία συγκεκριμένη περίπτωση επεξεργασίας προσωπικών δεδομένων που θα εμφανίζονταν ενώπιον της προκειμένου να αποφανθεί, αν αυτή είναι νόμιμη ή όχι.

Η Αρχή, κατά την επεξεργασία της παρούσας Οδηγίας, και για διευκόλυνση της κατανόησης της έννοιας του ν.2472/1997 στον ειδικό τομέα της εργασιακής σχέσης, έλαβε επίσης υπόψη τη Σύσταση (89) 2 του Συμβουλίου

της Ευρώπης για την προστασία των δεδομένων προσωπικού χαρακτήρα που χρησιμοποιούνται για σκοπούς απασχόλησης, καθώς και τον Κώδικα καλής πρακτικής (code of practice) του Διεθνούς Γραφείου Εργασίας για την προστασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων. Τα δύο αυτά κείμενα δεν είναι δεσμευτικού χαρακτήρα . Το τελευταίο μάλιστα δεν αναφέρεται σε υποχρεώσεις του νομοθέτη αλλά σε υποχρεώσεις του εργοδότη και η αναφορά στο εθνικό δίκαιο είναι έμμεση. Ωστόσο, παρά την έλλειψη δεσμευτικότητας, είναι σημαντικά κείμενα, καθώς κωδικοποιούν τόσο τα βασικά ζητήματα όσο και τις τάσεις σε αυτό το ιδιαίτερα ευαίσθητο πεδίο. Η Αρχή έλαβε επίσης σοβαρά υπόψη το σχετικό κείμενο εργασίας της Ευρωπαϊκής Επιτροπής που καταγράφει τις αρχικές σκέψεις της Επιτροπής και απευθύνεται στην Ομάδα 29 (Ομάδα που ιδρύθηκε με την κοινοτική Οδηγία 95/46/ΕΚ για την προστασία έναντι της επεξεργασίας προσωπικών δεδομένων και στην οποία συμμετέχουν οι εκπρόσωποι των εθνικών αρχών ελέγχου των χωρών της Ε.Ε.)

Σε περίπτωση που προκύψουν ερωτήματα ή προβλήματα ως προς την εφαρμογή του νόμου ή/ και της Οδηγίας αυτής είναι προφανές ότι η Αρχή – ήδη λόγω της αρμοδιότητάς της αλλά και με βάση τον τρόπο που αντιλαμβάνεται την αποστολή της – είναι στη διάθεση των ενδιαφερομένων, εργαζομένων και υπεύθυνων επεξεργασίας.

Β' ΑΝΤΙΚΕΙΜΕΝΟ –ΕΝΝΟΙΕΣ – ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ

1. Αντικείμενο της παρούσας Οδηγίας είναι η ερμηνεία των κανόνων του Ν. 2472/97 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και του Ν. 2774/99 για την προστασία των δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, προς τον σκοπό της ενιαίας εφαρμογής τους και η προσαρμογή τους στο πεδίο των σχέσεων απασχόλησης.

2. Ο νομοθέτης, με τον Ν. 2472/97, επέλεξε ορισμένες έννοιες, οι οποίες είναι σημαντικές για την κατανόηση και εφαρμογή του νόμου, και προσέδωσε σε αυτές δεσμευτικό νομοθετικό περιεχόμενο. Η Αρχή

θεωρεί χρήσιμο να **διευκρινίσει τις έννοιες αυτές σε σχέση με την** επεξεργασία και προστασία προσωπικών δεδομένων στο πεδίο των σχέσεων απασχόλησης.

- Ως εργαζόμενοι στην παρούσα Οδηγία νοούνται οι απασχολούμενοι τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα. Στην τελευταία περίπτωση, η Οδηγία βρίσκει εφαρμογή εφόσον πρόκειται για πρόσωπα που εργάζονται κατά τις οδηγίες και υπό τον έλεγχο του εργοδότη. Κρίσιμο στοιχείο για την εφαρμογή της Οδηγίας συνιστά δηλαδή η σχέση εξάρτησης μεταξύ προϊσταμένου/ εργοδότη και υπαλλήλου. Το κύρος της σχέσης απασχόλησης είναι αδιάφορο.
- Ως εργαζόμενοι κατά την παρούσα Οδηγία νοούνται επίσης α) οι υποψήφιοι για εργασία καθώς και β) οι πρώην εργαζόμενοι. Ως προς την πρώτη περίπτωση δεν συντρέχει μεν εξαρχής η σχέση εξάρτησης που χαρακτηρίζει την εργασιακή σχέση, ωστόσο είναι προφανές ότι κάποιος που αναζητεί εργασία βρίσκεται κατά κανόνα σε θέση που δεν του επιτρέπει να επιλέξει ελεύθερα ποια δεδομένα που τον αφορούν θα καταστήσει γνωστά και προσιτά σε τρίτους και άρα χρειάζεται αυξημένη προστασία. Στην περίπτωση των πρώην εργαζομένων είναι προφανές ότι η λύση της εργασιακής σχέσης δεν σημαίνει και αποδέσμευση από τους κανόνες νόμιμης και θεμιτής επεξεργασίας των προσωπικών δεδομένων. Περαιτέρω χρήση των δεδομένων θα μπορούσε να έχει δυσμενείς επιπτώσεις τόσο για την προστασία της προσωπικότητας και της ιδιωτικότητας όσο και για τα ιδιαίτερα έννομα συμφέροντα του πρώην εργαζομένου (π.χ. αναζήτηση νέας εργασίας κλπ.)
- Αντίστοιχα, ως εργοδότης (ή προϊστάμενος στην περίπτωση των δημοσίων αρχών) νοείται στην προκειμένη Οδηγία αυτός που προσδιορίζει δεσμευτικά την οργάνωση, το περιεχόμενο και γενικά τους όρους της εργασίας. Η Οδηγία απευθύνεται, ωστόσο, στους υπεύθυνους επεξεργασίας, ανεξαρτήτως εάν ταυτίζονται με τον εργοδότη ή προϊστάμενο. Αυτούς βαρύνει η συμμόρφωση προς τους γενικούς κανόνες επεξεργασίας των

προσωπικών δεδομένων, όπως αυτοί ερμηνεύονται και διευκρινίζονται στην παρούσα Οδηγία.

- Ως σκοποί επεξεργασίας που σχετίζονται με τη σχέση απασχόλησης και, κατά τούτο, δεν υπερβαίνουν ούτε περιγράφουν την αρχή του σκοπού (άρθρο 4 παρ. 1) νοούνται αυτοί που αφορούν την επιλογή και πρόσληψη του εργαζομένου, την εκπλήρωση της εργασιακής σχέσης και των εκατέρωθεν υποχρεώσεων που απορρέουν από αυτή, την εκτέλεση των σχετικών συμβάσεων, καθώς και την οργάνωση της εργασίας (καθορισμός των μέσων, μεθόδων, προτεραιοτήτων κλπ.).
- Έλεγχος και παρακολούθηση των εργαζομένων : Στην παρούσα Οδηγία ως έλεγχος και παρακολούθηση νοείται η χρήση μέσων παρακολούθησης, ιδίως ηλεκτρονικών υπολογιστών, κυκλωμάτων παρακολούθησης, ηχοσκόπησης, βιντεοσκόπησης, μεθόδων παρακολούθησης των επικοινωνιών ή των κινήσεων των εργαζομένων με σκοπό τον έλεγχο αυτών ή/και των χώρων και εγκαταστάσεων εργασίας.
- Βιομετρικές μέθοδοι: Ως βιομετρικές μέθοδοι νοούνται οι τεχνικές πιστοποίησης της ταυτότητας των εργαζομένων μέσω ανάλυσης σταθερών χαρακτηριστικών τους. Οι βιομετρικές μέθοδοι μπορούν να ταξινομηθούν σε δύο κατηγορίες: α) στις τεχνικές που στηρίζονται στην ανάλυση φυσικών ή γενετικών χαρακτηριστικών (όπως δακτυλικών αποτυπωμάτων, γεωμετρίας της παλάμης, ανάλυσης της κόρης του ματιού, των χαρακτηριστικών του προσώπου, του DNA) και β) στις τεχνικές που στηρίζονται στην ανάλυση συμπεριφοράς, όπως υπογραφής, φωνής, τρόπου πληκτρολόγησης.
- Χώροι εργασίας: Για τους σκοπούς της παρούσας Οδηγίας, ως χώρος εργασίας νοείται κάθε χώρος στον οποίο βρίσκεται εγκατεστημένος ο εργαζόμενος κατά την εκτέλεση της εργασίας που του έχει ανατεθεί. Η Αρχή προκρίνει αυτή την ευρεία ερμηνεία α) γιατί λαμβάνει υπόψη τόσο ιδιαίτερες μορφές εργασίας (π.χ. μεταφορές) όσο και τις τάσεις για ευέλικτες και

αποκεντρωμένες μορφές οργάνωσης της εργασίας (μορφές τηλεργασίας) και β) για να αποφευχθεί η περιγραφή των υποχρεώσεων και δεσμεύσεων του υπεύθυνου επεξεργασίας μέσω του στενού προσδιορισμού των χώρων εργασίας.

3. Πεδίο εφαρμογής - Δημόσιος και Ιδιωτικός τομέας/Γραφεία Εργασίας : Όπως προκύπτει και από την έννοια του εργαζόμενου στην παρούσα Οδηγία, η ερμηνεία και προσαρμογή των γενικών κανόνων αφορά αδιακρίτως τόσο τον ιδιωτικό όσο και το δημόσιο τομέα. Οι όροι εργασίας δημόσιων και ιδιωτικών υπαλλήλων δεν ταυτίζονται. Ωστόσο, η διάκριση ως προς την αντιμετώπιση ούτε δικαιολογείται ούτε κρίνεται αναγκαία, καθώς η επεξεργασία δεδομένων των απασχολούμενων και στους δύο τομείς παρουσιάζει τα ίδια βασικά χαρακτηριστικά (σχέση εξάρτησης, με διαφοροποιημένη πάντως ένταση λόγω του καθεστώτος μονιμότητας των δημοσίων υπαλλήλων) και αποβλέπει στους ίδιους κατά βάση σκοπούς (πρόσληψη, οργάνωση εργασίας, αξιολόγηση απασχολουμένων κλπ.). Διαφοροποιήσεις και αποκλίσεις μπορούν να γίνουν αποδεκτές με κριτήριο τη φύση και την ιδιαιτερότητα της εργασίας ή της σχέσης εργασίας, αλλά αυτό συμβαίνει ανεξάρτητα από την ένταξη στον ιδιωτικό ή τον δημόσιο τομέα. Εξάλλου η διάκριση δεν θα ήταν λειτουργική εξαιτίας α) της βαθμιαίας “ιδιωτικοποίησης” πολλών κρατικών δραστηριοτήτων ή αρμοδιοτήτων, καθώς και β) της εισαγωγής στον δημόσιο τομέα μορφών εργασίας που καταρχήν προσιδιάζουν στον ιδιωτικό.

4. Η παρούσα Οδηγία αφορά και την επεξεργασία δεδομένων προσωπικού χαρακτήρα που πραγματοποιείται από τα γραφεία ευρέσεως εργασίας και διαμεσολάβησης, τα γραφεία προσωρινής εργασίας, καθώς και τους συμβούλους επιλογής προσωπικού αφού, και στις περιπτώσεις αυτές, πραγματοποιείται συλλογή και επεξεργασία προσωπικών δεδομένων για σκοπούς απασχόλησης. Η επεξεργασία που διενεργούν τα γραφεία αυτά δεν υπολείπεται σε ένταση και βαθμό διείσδυσης στην ιδιωτική ζωή και προσβολής ατομικών δικαιωμάτων. Στην προκειμένη περίπτωση, μάλιστα, υπάρχει

ένας αόριστος και ανοιχτός αριθμός αποδεκτών των δεδομένων αυτών. Εξάλλου, η αναζήτηση εργασίας δημιουργεί, όπως προαναφέρθηκε, μια οιονεί σχέση εξάρτησης. Ως γραφεία ευρέσεως εργασίας νοούνται τόσο τα ιδιωτικά γραφεία όσο και οι δημόσιες υπηρεσίες που προσφέρουν δυνατότητες/θέσεις απασχόλησης (ΟΑΕΔ). Δεν συμπεριλαμβάνονται δημόσιες υπηρεσίες που διενεργούν διαγωνισμούς ή άλλες διαδικασίες επιλογής προσωπικού (π.χ. ΑΣΕΠ), καθώς, στην περίπτωση αυτή, δεν προσωποποιείται κατά κανόνα η σχέση μεταξύ υπευθύνου επεξεργασίας και υποκειμένου των δεδομένων, γι΄ αυτό και κρίνεται επαρκής η υπαγωγή στους γενικούς κανόνες.

5. Η παρούσα Οδηγία αφορά επίσης τα γραφεία και επιχειρήσεις που διαθέτουν εργαζόμενους σε άλλα φυσικά ή νομικά πρόσωπα (« δανεισμός »). Στην περίπτωση αυτή η Οδηγία ισχύει τόσο για τον αρχικό εργοδότη, ο οποίος έχει καταρτίσει τη σχετική σύμβαση, όσο και για τον ανάδοχο εργοδότη, στον οποίο κάθε φορά και κατά περίπτωση ο εργαζόμενος παρέχει τις υπηρεσίες του.

6. Εκτελούντες την επεξεργασία*:* Η παρούσα Οδηγία αφορά τέλος και κάθε τρίτο εκτελούντα τις σχετικές επεξεργασίες για λογαριασμό του υπευθύνου επεξεργασίας και για σκοπούς που εντάσσονται στο πεδίο των σχέσεων απασχόλησης.

Γ' ΓΕΝΙΚΕΣ ΑΡΧΕΣ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ

1. Η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων πρέπει να πραγματοποιείται με θεμιτά μέσα και με τρόπο ώστε να διασφαλίζεται ο σεβασμός της ιδιωτικής ζωής, της προσωπικότητας και της ανθρώπινης αξιοπρέπειας των εργαζομένων στον χώρο της εργασίας και, γενικότερα, στο πλαίσιο των εργασιακών σχέσεων . Όπως τονίζεται στο άρθρο 1 του Ν. 2472/97, η θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα

αποσκοπεί στην προστασία των δικαιωμάτων και θεμελιωδών ελευθεριών κάθε προσώπου.

2. Όπως προκύπτει από την αρχή του σκοπού, την οποία ο Έλληνας νομοθέτης καθιέρωσε ως κεντρική αρχή για την προστασία των προσωπικών δεδομένων, η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων επιτρέπεται αποκλειστικά για σκοπούς που συνδέονται άμεσα με τη σχέση απασχόλησης και εφ΄ όσον είναι αναγκαία για την εκπλήρωση των εκατέρωθεν υποχρεώσεων που θεμελιώνονται σε αυτή τη σχέση, είτε αυτές πηγάζουν από το νόμο είτε από σύμβαση.

3. Σύμφωνα με το άρθρο 4 παρ. 1 α του Ν. 2472/97, τα δεδομένα προσωπικού χαρακτήρα (των εργαζομένων) πρέπει να συλλέγονται και να υφίστανται επεξεργασία για σαφείς και καθορισμένους σκοπούς. Τόσο από τη διατύπωση της διάταξης αυτής, όσο και από την υποχρέωση ενημέρωσης των υποκειμένων, συνάγεται ότι οι σκοποί της επεξεργασίας θα πρέπει να είναι εκ των προτέρων γνωστοί στους εργαζομένους και κατανοητοί από αυτούς.

4. Η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα των εργαζομένων για σκοπούς που δεν αφορούν, άμεσα ή έμμεσα, τη σχέση απασχόλησης απαγορεύεται από την αρχή του σκοπού. Η συγκατάθεση των εργαζομένων δεν μπορεί να άρει την απαγόρευση της υπέρβασης του σκοπού. Δεν παραγνωρίζεται η ελευθερία της συγκατάθεσης, η οποία συνιστά εξάλλου τον κατά νόμο βασικό θεμελιωτικό λόγο της επεξεργασίας δεδομένων. Όπως όμως έχει κρίνει η Αρχή σε επιμέρους υποθέσεις, η νομιμότητα της επεξεργασίας αξιολογείται τόσο με βάση τη διαπίστωση της συνδρομής μιας ή περισσοτέρων βάσεων νομιμότητας (άρθρα 5 και 7 του Ν. 2472/97), όσο και κυρίως με βάση την τήρηση των γενικών αρχών που εισάγει το άρθρο 4. Εξάλλου, στην περίπτωση των σχέσεων απασχόλησης, η εγγενής ανισότητα των μερών και η κατά κανόνα σχέση εξάρτησης των εργαζομένων θέτει σε αμφιβολία την ελευθερία της συγκατάθεσης των εργαζομένων, στοιχείο απαραίτητο για την εγκυρότητά της επεξεργασίας,

όπως προκύπτει από τους γενικούς κανόνες του δικαίου αλλά και συγκεκριμένα από το συνδυασμό των άρθρων 2 στοιχ. ια, 5 παρ. 1 και 7παρ. 2α του νόμου για την προστασία προσωπικών δεδομένων.

5. Σύμφωνα με την αρχή της αναλογικότητας, όπως καθιερώνεται στο άρθρο 4 παρ. 1 β του Ν. 2472/97, τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από όσα κάθε φορά χρειάζονται ενόψει των σκοπών επεξεργασίας, στο πλαίσιο των σχέσεων απασχόλησης και της οργάνωσης της εργασίας. Τα δεδομένα πρέπει να είναι ακριβή και να υποβάλλονται σε ενημέρωση. Διατηρούνται όσο χρόνο απαιτείται για την εκπλήρωση των επιμέρους σκοπών επεξεργασίας. Σε περίπτωση λήξης της σχέσης απασχόλησης ή σε περίπτωση μη επιλογής /πρόσληψης, τα δεδομένα των εργαζομένων /υποψηφίων πρέπει να διατηρούνται σε μορφή που επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων μόνο για όσο διάστημα είναι αναγκαίο για την υπεράσπιση δικαιώματος ενώπιον δικαστηρίου. Περαιτέρω διατήρηση και επεξεργασία των δεδομένων αυτών είναι επιτρεπτή μόνον εφ΄ όσον προβλέπεται από νόμο που συνάδει με τον Ν. 2472/97 ή εάν το ζητήσει ρητά ο εργαζόμενος /υποψήφιος για τον σκοπό της μελλοντικής αναζήτησης θέσης απασχόλησης, ή νέας απασχόλησης, ή για χρήση από τον ίδιο τον εργαζόμενο (για την βεβαίωση εργασίας και γενικά την αναγνώριση και θεμελίωση δικαιωμάτων του εργαζομένου).

6. Είναι αυτονόητο ότι παραίτηση του εργαζομένου από τα δικαιώματα που εισάγει ο Ν. 2472/97 είναι άκυρη. Εξάλλου η άσκηση των δικαιωμάτων που προβλέπονται από το ν.2472/1997 (γνωστοποίησης, πρόσβασης, αντίρρησης κ.λπ.) δεν μπορεί σε καμία περίπτωση να έχει δυσμενείς συνέπειες για τον εργαζόμενο, αφού έτσι θα αναιρούνταν ο σκοπός του νόμου. Για παράδειγμα η άσκηση του δικαιώματος πρόσβασης ή και η προσφυγή στην Αρχή για να παράσχει τη συνδρομή της στην άσκηση των δικαιωμάτων του δεν μπορεί να οδηγεί σε δυσμενή αξιολόγηση του εργαζόμενου, σε καταγγελία της συμβάσεως/σχέσης εργασίας κλπ.

7. Όπως προκύπτει και από το άρθρο 14 του Ν. 2472/97 αποφάσεις που αφορούν κάθε πτυχή της προσωπικότητας των εργαζομένων, όπως η συμπεριφορά ή η αποδοτικότητά τους, δεν επιτρέπεται να λαμβάνονται αποκλειστικά βάσει αυτοματοποιημένης επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Μία τέτοια διαδικασία θα υποβίβαζε τους εργαζόμενους σε πληροφοριακά αντικείμενα και θα πρόσβαλλε την προσωπικότητά τους.

8. Δεδομένα προσωπικού χαρακτήρα που συλλέγονται σε συνδυασμό με τεχνικά ή οργανωτικά μέτρα προκειμένου να διασφαλιστεί η ορθή και ασφαλής λειτουργία συστημάτων δεν μπορεί να χρησιμοποιηθούν για τον έλεγχο της συμπεριφοράς των εργαζομένων, εκτός εάν αυτή συνδέεται με τη λειτουργία των συστημάτων αυτών. Χαρακτηριστικό παράδειγμα της τελευταίας περίπτωσης συνιστά η καταγραφή ενεργειών, συνομιλιών κλπ. των πιλότων στο λεγόμενο «μαύρο κουτί» ενός αεροσκάφους ή η καταγραφή συνομιλιών μεταξύ πιλότων και πύργου ελέγχου.

Δ' ΣΥΛΛΟΓΗ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ

1. Λόγω της ιδιαίτερης σχέσης εξάρτησης στην οποία υπόκεινται οι εργαζόμενοι ή οι υποψήφιοι, ο υπεύθυνος επεξεργασίας θα πρέπει να απευθύνεται στους ίδιους για να συλλέξει τα δεδομένα προσωπικού χαρακτήρα που τους αφορούν.

2. Η συλλογή δεδομένων προσωπικού χαρακτήρα που αφορούν τον εργαζόμενο ή τον υποψήφιο από τρίτους είναι ανεκτή, υπό το πρίσμα του άρθρου 4 παρ. 1 και του άρθρου 5 παρ. 2 α, β, και ε, μόνον εφ΄ όσον είναι αναγκαία για την εκπλήρωση του επιδιωκόμενου σκοπού. Έτσι, ενώ η αναζήτηση πληροφοριών για μία βρεφοκόμο ή για έναν ταμία από προηγούμενο εργοδότη θα ήταν ενδεχομένως θεμιτή - υπό την επιφύλαξη βέβαια των τυχόν ειδικών συνθηκών – δεν μπορεί π.χ. να κριθεί ως

εμπίπτουσα στις προϋποθέσεις επιτρεπτής επεξεργασίας η αναζήτηση πληροφοριών από γείτονες ή συγχωριανούς για τις συνήθειες διασκέδασης ή για τις πολιτικές πεποιθήσεις ενός προσώπου. Βασική προϋπόθεση θεωρείται η προηγούμενη ενημέρωση του εργαζομένου ή του υποψηφίου για πρόσληψη ότι πρόκειται να αναζητηθούν πληροφορίες για το πρόσωπό του από τρίτους και η ρητή συγκατάθεση του. Αυτός που προτίθεται να ζητήσει πληροφορίες από τρίτους οφείλει να ενημερώσει τον εργαζόμενο ή τον υποψήφιο για τους σκοπούς της συλλογής και επεξεργασίας, τις πηγές από τις οποίες θα ζητήσει πληροφορίες, το είδος των δεδομένων καθώς και τις συνέπειες της πιθανής άρνησης της συγκατάθεσης.

3. Επισημαίνεται ότι, κατά τη διαδικασία επιλογής, η συλλογή δεδομένων προσωπικού χαρακτήρα που αφορούν τους υποψήφιους θα πρέπει να περιορίζεται στα δεδομένα που είναι απολύτως αναγκαία για να εκτιμηθούν η καταλληλότητα και οι ικανότητες των υποψηφίων για τη συγκεκριμένη θέση. Η Αρχή τονίζει ότι η επισήμανση αυτή αφορά πολύ περισσότερο τα γραφεία ευρέσεως εργασίας, τα γραφεία διαμεσολάβησης κλπ., δεδομένου ότι στην περίπτωση αυτή δεν δημιουργείται ούτε πρόκειται να δημιουργηθεί μία μονιμότερη σχέση εμπιστοσύνης, όπως είναι η σχέση απασχόλησης που συνδέει τον εργαζόμενο με τον εργοδότη/ προϊστάμενο.

4. Έχει διαπιστωθεί ότι, στις σύγχρονες μεθόδους επιλογής προσωπικού, συγκαταλέγεται η διενέργεια εξετάσεων, αναλύσεων ή συναφών διαδικασιών για την εκτίμηση των προσόντων, ικανοτήτων και δεξιοτήτων του υποψηφίου. Συχνά μάλιστα οι εξετάσεις και αναλύσεις αυτές αποσκοπούν στην αξιολόγηση του χαρακτήρα και της προσωπικότητας του υποψηφίου. Τέτοιες εξετάσεις ή αναλύσεις συνιστούν μία βαθιά διείσδυση στην προσωπικότητα και στην ιδιωτική ζωή του υποψηφίου για μία θέση εργασίας, για μία προαγωγή κλπ.. Οι εξετάσεις και αναλύσεις αυτές μπορεί να αποκαλύπτουν ή να παραπέμπουν σε πτυχές της προσωπικότητας που άπτονται των πεποιθήσεων, των συνηθειών ή και της ψυχικής ή διανοητικής υγείας /κατάστασης ενός ανθρώπου. Για τους λόγους αυτούς, η αρχή της αναλογικότητας επιτάσσει να διεξάγονται τέτοιες εξετάσεις ή αναλύσεις μόνο σε εξαιρετικές περιπτώσεις και μόνον εφ΄ όσον αυτό είναι

απολύτως αναγκαίο και πρόσφορο για την επίτευξη ειδικού σκοπού που συνδέεται άμεσα με τη συγκεκριμένη σχέση /θέση απασχόλησης και την επιλογή που σχετίζεται με αυτήν. Λόγω της φύσεως των δεδομένων, η συλλογή τους είναι κατά νόμο επιτρεπτή μόνο με την γραπτή συγκατάθεση του υποψηφίου, και αφού αυτός ενημερωθεί μεταξύ άλλων για την μέθοδο, τα κριτήρια, τους σκοπούς και τους (πιθανούς) αποδέκτες των αναλύσεων και των αποτελεσμάτων τους. Ο υποψήφιος πρέπει να ενημερώνεται και για τα αποτελέσματα. Τα δεδομένα αυτά διαγράφονται ή καταστρέφονται μόλις εκπληρωθεί ο σκοπός της συλλογής, εκτός εάν ο υποψήφιος ζητήσει ρητά τη διατήρησή τους

5. Ο ν.2472/97 έχει εισαγάγει ως κανόνα την απαγόρευση της επεξεργασίας των ευαίσθητων δεδομένων. Υπενθυμίζεται ότι η εξαίρεση που εισήγαγε ο Ν. 2819/00 (όπως τροποποιήθηκε με τον πρόσφατο Ν. 2915/01) σε σχέση με την απαλλαγή από την υποχρέωση γνωστοποίησης ή αίτησης για άδεια δεν απαλλάσσει από την υποχρέωση τήρησης των ουσιαστικών επιταγών του νόμου. Για ορισμένες θέσεις εργασίας είναι απαραίτητη η συλλογή και επεξεργασία δεδομένων που αφορούν τις ποινικές διώξεις και καταδίκες ενός προσώπου. Επισημαίνεται πάντως ότι η συλλογή και επεξεργασία είναι θεμιτή και νόμιμη μόνο εφόσον το είδος των δεδομένων αυτών συνδέεται άμεσα με την συγκεκριμένη απασχόληση και είναι απολύτως απαραίτητα για τη λήψη συγκεκριμένης απόφασης στο συγκεκριμένο πλαίσιο (π.χ. ποινικό μητρώο για εργαζόμενους που διαχειρίζονται χρήματα, για εκπαιδευτικούς κλπ.) Λόγω της φύσεως των δεδομένων αυτών και του βαθμού προσβολής που ενέχει η χρήση τους, αυτά πρέπει να συλλέγονται απευθείας και μόνον από τον εργαζόμενο ή τον υποψήφιο.

6. Ὅσον αφορά τα δεδομένα προσωπικού χαρακτήρα που αφορούν την υγεία του εργαζόμενου ή του υποψηφίου - λόγω της φύσης τους και των συνεπειών που μπορεί να έχει η αποκάλυψή τους – πρέπει να συλλέγονται απευθείας και μόνον από τους εργαζόμενους ή τους υποψήφιους και μόνον εφ΄ όσον αυτό είναι απολύτως απαραίτητο α) για την αξιολόγηση της καταλληλότητας του εργαζόμενου ή του υποψηφίου για μία συγκεκριμένη θέση ή εργασία, παρούσα ή μελλοντική (π.χ. εξετάσεις

για τους εργαζόμενους σε παιδικούς σταθμούς, εστιατόρια, ξενοδοχειακές επιχειρήσεις, οδηγούς, πιλότους κλπ.), β) για την εκπλήρωση των υποχρεώσεων του εργοδότη για υγιεινή και ασφάλεια της εργασίας και γ) για τη θεμελίωση δικαιωμάτων των εργαζομένων και αντίστοιχη απόδοση κοινωνικών παροχών.

7. Διαπιστώνεται τελευταία διεθνής τάση να εισαχθούν οι γενετικές εξετάσεις στο πεδίο των εργασιακών σχέσεων. Όπως έχει αποφανθεί η Αρχή, η ανάλυση του γενετικού υλικού ενός ανθρώπου συνιστά ουσιώδη και ριζική προσβολή της προσωπικότητάς του, καθώς αποκαλύπτει στοιχεία για το παρελθόν αλλά και το μέλλον του (κληρονομικότητα, προδιάθεση για ασθένειες κλπ.). Η Αρχή διατυπώνει την ανησυχία της για το ενδεχόμενο να χρησιμοποιηθούν τα στοιχεία που απορρέουν από τέτοιες εξετάσεις για τη δυσμενή διάκριση και μεταχείριση των εργαζομένων. Η ένταση της προσβολής είναι τέτοια που, κατά την αληθινή έννοια του ν.2472/1997, η διενέργεια γενετικών εξετάσεων για σκοπούς που σχετίζονται με την σχέση απασχόλησης απαγορεύεται απολύτως υπό το παρόν νομοθετικό καθεστώς, ως αντιβαίνουσα στην αρχή της αναλογικότητας, λαμβανομένης υπόψη και της συνταγματικά προστατευόμενης αξίας του ανθρώπου. Η ύπαρξη συγκατάθεσης, με δεδομένες τις σοβαρές επιφυλάξεις για την πραγματική ελευθερία της συγκατάθεσης στο πεδίο των εργασιακών σχέσεων, δεν θεραπεύει την αντίθεση προς την αρχή της αναλογικότητας. Γενετικές εξετάσεις για τους σκοπούς αυτούς είναι επιτρεπτές μόνον με βάση ρητή και ειδική διάταξη νόμου. Ειδικότερα, η συνταγματική προστασία της αξίας, της προσωπικότητας, των προσωπικών δεδομένων, και της γενετικής ταυτότητας του ανθρώπου αλλά και της εργασίας, όπως διατυπώνονται μάλιστα στο Σύνταγμα μετά την πρόσφατη αναθεώρησή του (νέα άρθρα 2§1, 9^{A}, 5 §5), επιβάλλει de lege ferenda, σε περίπτωση εισαγωγής νομοθεσίας επιτρέπουσας την ανάλυση του γενετικού υλικού, την ταυτόχρονη θέσπιση ειδικών προϋποθέσεων και εγγυήσεων όπως π.χ.: α) διενέργεια τέτοιων εξετάσεων μόνο για την προστασία της υγείας του εργαζόμενου και υπό την προϋπόθεση ότι ο σκοπός αυτός δεν μπορεί να επιτευχθεί με ηπιότερο μέσο, β) ειδική προηγούμενη ενημέρωση του εργαζομένου από ιατρό, γ) διενέργεια των γενετικών εξετάσεων μόνον από

δημόσιους φορείς, δ) ειδική προηγούμενη άδεια της Αρχής Προστασίας Προσωπικών Δεδομένων.

Ε' ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ ΑΠΟ ΤΗ ΧΡΗΣΗ ΣΥΣΤΗΜΑΤΩΝ ΕΛΕΓΧΟΥ ΚΑΙ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ

1. Η Αρχή έχει διαπιστώσει ότι σε πολλές επιχειρήσεις και υπηρεσίες γίνεται χρήση μέσων ελέγχου και παρακολούθησης των χώρων αλλά, σε τελευταία ανάλυση, και των ίδιων των εργαζομένων. Συστήματα ελέγχου της πρόσβασης, βιντεοπαρακολούθηση, έλεγχος των τηλεφωνημάτων, είναι ορισμένα από αυτά τα μέσα. Η χρήση των μέσων αυτών και των μεθόδων που οδηγούν στη συλλογή και επεξεργασία προσωπικών δεδομένων υπόκειται στους όρους των Ν. 2472/97 και Ν. 2774/99 και κρίνεται με βάση τις ειδικότερες επιταγές τους. Οι μέθοδοι ελέγχου και παρακολούθησης και ο σκοπός που εξυπηρετούν δεν επιτρέπεται να προσβάλλουν την ανθρώπινη αξιοπρέπεια, σύμφωνα με τις προαναφερθείσες διατάξεις του Συντάγματος και του ν.2472/1997. Η συλλογή δεδομένων προσωπικού χαρακτήρα με τη χρήση μεθόδων ελέγχου και παρακολούθησης των εργαζομένων πρέπει να περιορίζεται στα δεδομένα που συνδέονται άμεσα με τη σχέση απασχόλησης και να μην επεκτείνεται κατά το δυνατόν στην προσωπική συμπεριφορά, στα προσωπικά χαρακτηριστικά ή στις προσωπικές εσωτερικές και εξωτερικές επαφές των εργαζομένων. Πρέπει επίσης να προβλέπεται η ύπαρξη χώρων που δεν ελέγχονται ούτε παρακολουθούνται, καθώς και η διάθεση προσιτών στους εργαζόμενους τηλεπικοινωνιακών μέσων για τις προσωπικές επικοινωνίες τους.

2. Η αρχή του σκοπού επιβάλλει τη μη χρησιμοποίηση για άλλους σκοπούς των δεδομένων προσωπικού χαρακτήρα που προκύπτουν από τη χρήση ηλεκτρονικών ή άλλων καρτών για τον έλεγχο της πρόσβασης στον χώρο εργασίας.

3. Σε σχέση με τη χρήση βιομετρικών μεθόδων, η Αρχή έχει αποφανθεί ότι, ιδίως ορισμένες από αυτές, θίγουν κατάφωρα την ανθρώπινη αξιοπρέπεια και την προσωπικότητα. (Υπενθυμίζεται η απόφασή της για τη χρήση δακτυλικών αποτυπωμάτων για τον έλεγχο της προσέλευσης στην εργασία) . Από την αρχή της αναλογικότητας, όπως αυτή προβλέπεται στο άρθρο 4 του Ν. 2472/97, η χρήση βιομετρικών μεθόδων για τη διαπίστωση της ταυτότητας των εργαζομένων και την πρόσβαση στο σύνολο ή τμήμα των χώρων εργασίας είναι επιτρεπτή μόνο στις περιπτώσεις που αυτό επιβάλλεται από ιδιαίτερες απαιτήσεις ασφαλείας των χώρων εργασίας και εφόσον δεν υπάρχει άλλο μέσο για την επίτευξη του σκοπού αυτού (π.χ. στρατιωτικές εγκαταστάσεις, εργαστήρια υψηλού κινδύνου) . Κατά συνέπεια, ο υπεύθυνος επεξεργασίας οφείλει να σταθμίζει κάθε φορά αφενός τους υπάρχοντες κινδύνους, την έκταση των κινδύνων αυτών και τις υπάρχουσες εναλλακτικές δυνατότητες αντιμετώπισης των κινδύνων και, αφετέρου, τις προσβολές της ανθρώπινης προσωπικότητας και της ιδιωτικότητας από τη χρήση τέτοιων μεθόδων.

4. Η Αρχή έχει δεχθεί καταγγελίες που αφορούν τον έλεγχο των επικοινωνιών των εργαζομένων. Η ένταση του ελέγχου αυτού ποικίλλει, ξεκινώντας από τον έλεγχο του κόστους έως τη διακρίβωση του περιεχομένου και της επαγγελματικής ή ιδιωτικής φύσης της επικοινωνίας. Όπως επιτάσσει και το άρθρο 5 παρ. 5 του Ν. 2774/99, οι εργαζόμενοι ενημερώνονται εκ των προτέρων για την αποστολή αναλυτικών λογαριασμών στον συνδρομητή για τις τηλεπικοινωνιακές υπηρεσίες των οποίων κάνουν χρήση στον χώρο εργασίας ή/και σε σχέση με αυτή. Η συλλογή και επεξεργασία δεδομένων που αφορούν τις εισερχόμενες και εξερχόμενες κλήσεις και γενικά επικοινωνίες (στις οποίες συμπεριλαμβάνεται και το ηλεκτρονικό ταχυδρομείο) στον χώρο εργασίας επιτρέπεται εφ΄ όσον είναι απολύτως αναγκαία για την οργάνωση και τον έλεγχο της διεκπεραίωσης της συγκεκριμένης εργασίας ή του κύκλου εργασιών και ιδίως τον έλεγχο των δαπανών. Τα στοιχεία της επικοινωνίας που καταχωρίζονται πρέπει να περιορίζονται στα απολύτως απαραίτητα και πρόσφορα δεδομένα για την επίτευξη των σκοπών αυτών. Σε καμία δεν επιτρέπεται η καταχώριση και επεξεργασία ολόκληρου του αριθμού ή του συνόλου των στοιχείων της

επικοινωνίας ούτε στοιχείων από το περιεχόμενό τους, τα οποία – υπενθυμίζεται – δεν επιτρέπεται να συλλεγούν παρά μόνον με άδεια της δικαστικής Αρχής και εφ΄ όσον τούτο επιβάλλεται για λόγους εθνικής ασφάλειας ή για την διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων (άρθρο 19Σ., ν.2225/1994 Α΄121). Το άρθρο 5§3 του ν.2774/1999 ορίζει εξάλλου ότι, εφ΄ όσον το ζητήσει ο συνδρομητής ή ο χρήστης, ο φορέας παροχής τηλεπικοινωνιακού δικτύου ή και διαθέσιμης στο κοινό υπηρεσίας, οφείλει να διαγράψει τα τρία τελευταία ψηφία των κληθέντων αριθμών. Η διάταξη αυτή συνδυάζεται με την προαναφερθείσα §5 του ίδιου άρθρου, αλλά και κυρίως με την ισχύουσα κατά την επεξεργασία των προσωπικών δεδομένων, αρχή της αναλογικότητας, από την οποία επιβάλλεται στον συνδρομητή, όταν είναι εργοδότης, και η τηλεπικοινωνιακή υπηρεσία βρίσκεται στο χώρο εργασίας και είναι προσιτή και στον εργαζόμενο, να ζητήσει από τον φορέα την διαγραφή των τριών τελευταίων αριθμών. Τούτο έχει κριθεί ήδη από την Αρχή με απόφασή της.

5. Η Αρχή έχει καταγράψει περιπτώσεις στις οποίες λαμβάνει χώρα συλλογή και επεξεργασία δεδομένων που σχετίζονται με τις επισκέψεις των εργαζομένων σε ιστοχώρους και ιστοσελίδες. Η αρχή του σκοπού και της αναλογικότητας, όπως αυτές καθιερώνονται στον νόμο και έχουν ερμηνευτεί από την Αρχή, επιβάλλουν μόνο την μεμονωμένη και κατ' εξαίρεση συλλογή και επεξεργασία τέτοιων δεδομένων και εφόσον αυτό θεμελιώνεται σε ένα προφανές υπέρτερο έννομο συμφέρον του υπευθύνου επεξεργασίας (άρθρο 5 παρ. 2 ε). Ένα τέτοιο έννομο συμφέρον μπορεί να συντρέχει όταν τεκμηριώνεται η ανάγκη εξακρίβωσης συμπεριφορών που απαγορεύονται από τις ρυθμίσεις που διέπουν τη σχέση απασχόλησης ή από κανονισμούς εργασίας, π.χ. επίσκεψη σε ιστοχώρους και ιστοσελίδες με πορνογραφικό περιεχόμενο. Από την αρχή της αναλογικότητας απορρέει επίσης η απαγόρευση της γενικής, συστηματικής και προληπτικής συλλογής και καταχώρισης των δεδομένων που αφορούν τις επισκέψεις που αναφέρονται παραπάνω. Κρίσιμο στοιχείο για την κρίση του επιτρεπτού μιας τέτοιας συλλογής και καταχώρισης συνιστά η ειδική ενημέρωση των εργαζομένων για τη συλλογή και

επεξεργασία τέτοιων δεδομένων, ενημέρωση η οποία εξάλλου επιτάσσεται ρητώς από τις γενικές διατάξεις (βλ. Άρθρο 11 του Ν. 2472/97).

6. Η εισαγωγή και χρήση (κλειστών) κυκλωμάτων παρακολούθησης, ηχοσκόπησης, βιντεοσκόπησης και άλλων συναφών συστημάτων έχει απασχολήσει κατ΄ επανάληψη την Αρχή. Η χρήση τέτοιων συστημάτων στους χώρους εργασίας επιτρέπεται εφ΄ όσον είναι αναγκαία για την ασφάλεια των χώρων εργασίας, την προστασία των προσώπων, εργαζομένων και μη, που βρίσκονται στους χώρους αυτούς καθώς και την προστασία περιουσιακών αγαθών. Ο υπεύθυνος επεξεργασίας οφείλει να σταθμίζει κάθε φορά αφενός τους υπάρχοντες κινδύνους, την έκταση των κινδύνων αυτών, τις υπάρχουσες εναλλακτικές δυνατότητες αντιμετώπισης των κινδύνων αυτών και, αφετέρου, τις προσβολές της ανθρώπινης προσωπικότητας και της ιδιωτικότητας από τη χρήση τέτοιων μεθόδων. Η αρχή του σκοπού επιτάσσει τη μη χρήση δεδομένων που έχουν συλλεγεί για τους παραπάνω σκοπούς ως αποκλειστικά κριτήρια για την αξιολόγηση της συμπεριφοράς και της αποδοτικότητας των εργαζομένων. Επισημαίνεται, τέλος, ότι τα δεδομένα που συλλέγονται μέσω αυτών των κυκλωμάτων πολλές φορές δεν είναι ακριβή, μεταξύ των άλλων και για τεχνικούς λόγους. Ως εκ τούτου τα δεδομένα αυτά πρέπει να χρησιμοποιούνται αφού προηγουμένως επιβεβαιωθεί η ακρίβειά τους.

7. Ο διαρκής έλεγχος των χώρων εργασίας με μέσα παρακολούθησης προσβάλλει την αξιοπρέπεια και την ιδιωτικότητα των εργαζομένων. Η βαρύτητα της προσβολής επιβάλλει ο διαρκής έλεγχος να γίνεται μόνο εφ΄ όσον αυτό δικαιολογείται από τη φύση και τις συνθήκες της εργασίας και είναι απαραίτητο για την προστασία της υγείας και της ασφάλειας των εργαζομένων και της ασφάλειας των χώρων εργασίας (στρατιωτικές εγκαταστάσεις, τράπεζες, εργοστάσια με εγκαταστάσεις υψηλού κινδύνου) . Δεδομένα που έχουν συλλεγεί για τους παραπάνω σκοπούς δεν επιτρέπεται να χρησιμοποιηθούν ως αποκλειστικά κριτήρια για την αξιολόγηση της συμπεριφοράς και της αποδοτικότητας των εργαζομένων.

8. Όπως επιτάσσεται και από την υποχρέωση ενημέρωσης που έχει εισαγάγει ο νομοθέτης με το άρθρο 11 του Ν. 2472/97, οι εργαζόμενοι πρέπει να ενημερώνονται για την εισαγωγή και χρήση μεθόδων ελέγχου και παρακολούθησης και ιδίως για τον σκοπό για τον οποίο απαιτούνται τα δεδομένα που συλλέγονται με τη χρήση αυτών των μεθόδων, τα βασικά τεχνικά χαρακτηριστικά των μεθόδων, τα πρόσωπα στα οποία τα δεδομένα αυτά διαβιβάζονται ή ενδέχεται να διαβιβαστούν και τα δικαιώματα των εργαζομένων. Τα δεδομένα προσωπικού χαρακτήρα που προκύπτουν από τη χρήση μεθόδων ελέγχου και παρακολούθησης δεν μπορεί να χρησιμοποιηθούν εις βάρος του εργαζομένου, εάν αυτός δεν έχει προηγουμένως ενημερωθεί για την εισαγωγή των μεθόδων ελέγχου και παρακολούθησης και για την χρήση των δεδομένων αυτών. Λόγω της φύσεως της σχέσεως απασχόλησης αλλά και της έντασης της προσβολής, κατά ορθή εφαρμογή του νόμου, οι εκπρόσωποι των εργαζομένων πρέπει να ενημερώνονται και να διατυπώνουν γνώμη πριν από την εισαγωγή μεθόδων ελέγχου και παρακολούθησης των εργαζομένων.

ΣΤ' ΕΠΕΞΕΡΓΑΣΙΑ ΚΑΙ ΧΡΗΣΗ ΤΩΝ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ

1. Η επεξεργασία και χρήση των δεδομένων προσωπικού χαρακτήρα των εργαζομένων διέπεται από τους κανόνες του Ν. 2472/97.
2. Τα δεδομένα υγείας ή άλλα ευαίσθητα προσωπικά δεδομένα των εργαζομένων (όπως τα δεδομένα που αφορούν ποινικές διώξεις κλπ.) πρέπει να καταχωρίζονται και να διατηρούνται χωριστά από τα άλλα δεδομένα.
3. Πρόσβαση στους ατομικούς φακέλους και γενικά στα δεδομένα προσωπικού χαρακτήρα των εργαζομένων μπορούν να έχουν μόνον οι ίδιοι, ο υπεύθυνος επεξεργασίας και τα ειδικά προς τούτο εξουσιοδοτημένα από αυτόν πρόσωπα.
4. Τα δεδομένα προσωπικού χαρακτήρα των εργαζομένων δεν πρέπει να καταχωρίζονται ή να κωδικοποιούνται με τρόπο ώστε να μην είναι αντιληπτά στους εργαζόμενους ή να επιτρέπουν κάθε είδους

χαρακτηρισμό ή την δημιουργία μορφότυπων των εργαζομένων, χωρίς τη γνώση των τελευταίων.

Ζ' ΔΙΑΒΙΒΑΣΗ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ

1. Ένας από τους μείζονες κινδύνους για τα δικαιώματα των εργαζομένων εντοπίζεται στη διαβίβασή των προσωπικών δεδομένων τους σε τρίτα πρόσωπα και στην περαιτέρω χρήση των δεδομένων αυτών είτε για διαφορετικούς σκοπούς είτε σε διαφορετικά περιβάλλοντα. Σύμφωνα με τις αρχές του άρθρου 4 του Ν. 2472/97, σε συνδυασμό με τη ρύθμιση του άρθρου 7^{A} παρ. $1^{α}$, τα δεδομένα προσωπικού χαρακτήρα των εργαζομένων μπορεί να διαβιβάζονται ή να κοινοποιούνται σε τρίτους μόνο για σκοπούς που σχετίζονται άμεσα με τη σχέση απασχόλησης ή εφόσον η διαβίβαση προβλέπεται από νόμο που συνάδει με τα οριζόμενα στο Ν. 2472/97. (π.χ. διαβίβαση σε ασφαλιστικούς οργανισμούς). Επισημαίνεται ότι, και στην περίπτωση της διαβίβασης ή της κοινοποίησης, που συνιστούν άλλωστε μορφές επεξεργασίας, η συγκατάθεση των εργαζομένων δεν μπορεί να άρει την απαγόρευση της υπέρβασης του σκοπού

2. Με την επιφύλαξη ειδικών διατάξεων νόμου ή συλλογικών συμβάσεων εργασίας, η διαβίβαση δεδομένων προσωπικού χαρακτήρα των εργαζομένων στα συνδικαλιστικά τους όργανα επιτρέπεται μόνον εφ΄ όσον αυτά είναι απαραίτητα για άσκηση των συνδικαλιστικών δικαιωμάτων και μόνον στο μέτρο που αυτό είναι αναγκαίο.

3. Οι κανόνες για την διαβίβαση ή κοινοποίηση δεδομένων προσωπικού χαρακτήρα εφαρμόζονται, άλλωστε, και εντός της εργασιακής μονάδας/ εντός της εργασίας. Στην περίπτωση αυτή επιτρέπεται μόνο προς πρόσωπα ειδικά προς τούτο εξουσιοδοτημένα από τον υπεύθυνο

επεξεργασίας και μόνο στο πλαίσιο και στο μέτρο που αυτό είναι αναγκαίο για την εκπλήρωση ειδικού καθήκοντος ή ειδικά προσδιορισμένης εργασίας που έχει ανατεθεί στα πρόσωπα αυτά.

4. Ειδικότερα, η διαβίβαση δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία των εργαζομένων εντός της εργασιακής μονάδας επιτρέπεται μόνον σε ό,τι αφορά τα πορίσματα και εφ΄ όσον και στο μέτρο που αυτή είναι απολύτως απαραίτητη για την προστασία της υγείας των εργαζομένων, τη διαμόρφωση κρίσεων για την καταλληλότητά τους προς ανάληψη εργασίας, παρούσας ή μελλοντικής, ή για τη διαμόρφωση των συνθηκών εργασίας.

5. Υπενθυμίζεται ότι η διαβίβαση δεδομένων προσωπικού χαρακτήρα των εργαζομένων σε τρίτες χώρες, δηλ. σε χώρες που δεν ανήκουν στην Ευρωπαϊκή ΄Ένωση, υπόκειται στις ρυθμίσεις του Ν. 2472/97 αλλά και στους κανόνες και περιορισμούς που ισχύουν κάθε φορά με βάση την κοινοτική και εθνική νομοθεσία ή τις σχετικές κοινοτικές αποφάσεις (βλ. αποφάσεις της Ευρωπαϊκής Επιτροπής για την ύπαρξη ικανοποιητικού επιπέδου προστασίας, Safe Harbour Principles) για τη διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτες χώρες. Οι κανόνες και περιορισμοί αυτοί ισχύουν ακόμη και εάν τα δεδομένα προσωπικού χαρακτήρα των εργαζομένων διαβιβάζονται σε μητρικές, θυγατρικές ή συνδεδεμένες επιχειρήσεις, που έχουν την έδρα τους σε τρίτη χώρα.

Η' ΔΙΚΑΙΩΜΑΤΑ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ

Τα δικαιώματα των εργαζομένων έναντι του υπεύθυνου επεξεργασίας ορίζονται με σαφήνεια στα άρθρα 11-14 του ν.2472/1997. Αναγνωρίζεται στον εργαζόμενο το δικαίωμα ενημέρωσης (άρθρο 11), το δικαίωμα πρόσβασης (άρθρο 12), το δικαίωμα αντίρρησης (άρθρο 13) και το δικαίωμα προσωρινής δικαστικής προστασίας (άρθρο 14) :

1. <u>Το Δικαίωμα ενημέρωσης</u>

   Ναι μεν, όπως ήδη αναφέρθηκε, ο υπεύθυνος επεξεργασίας, τηρώντας του όρους του νόμου, όπως αυτοί έχουν ήδη αναλυθεί, έχει το δικαίωμα να

προβεί σε συλλογή και αρχειοθέτηση προσωπικών δεδομένων του εργαζόμενου, οφείλει, όμως, με τρόπο κατανοητό να τον ενημερώνει τουλάχιστον για τα εξής στοιχεία : α) την ταυτότητα του ίδιου και του εκπροσώπου του που διαχειρίζεται τα στοιχεία αυτά, β) το σκοπό της επεξεργασίας, ότι δηλαδή αυτή γίνεται στο πλαίσιο της οργάνωσης της εργασιακής σχέσης και αποβλέπει μόνο σ' αυτή, γ) τους αποδέκτες και τις κατηγορίες αποδεκτών των δεδομένων, τα φυσικά, δηλαδή ή νομικά πρόσωπα ή δημόσιες αρχές ή υπηρεσίες ή άλλους οργανισμούς, στους οποίους ανακοινώνονται ή μεταδίδονται τα δεδομένα. Πρέπει εδώ να σημειωθεί ότι οι αποδέκτες αυτοί, ανεξάρτητα από το αν είναι τρίτοι ή όχι, πρέπει να προκύπτουν είτε από το νόμο είτε από τη σύμβαση. Επομένως, ο εργοδότης δεν μπορεί αυθαίρετα να ορίσει αποδέκτες και να ενημερώνει περί αυτών τον εργαζόμενο αφού το δικαίωμα της αποστολής σε τρίτους των δεδομένων είναι συμφυές με το νόμο και τη σύμβαση, η έρευνα δε της νομιμότητας του, προηγείται του ελέγχου της ενημέρωσης. Το δικαίωμα ενημέρωσης πάντως υφίσταται ανεξάρτητα από τη νομιμότητα της αποστολής των δεδομένων σε τρίτους. Ο υπεύθυνος επεξεργασίας οφείλει τέλος δ) να ενημερώνει τον εργαζόμενο ότι έχει το δικαίωμα πρόσβασης. Δεδομένου ότι, όπως έχει ήδη αναφερθεί, στη σχέση εργασίας, ο υπεύθυνος επεξεργασίας ζητεί πάντοτε (εκτός των περιπτώσεων που ορίζει διαφορετικά ο νόμος) τη συνδρομή του εργαζόμενου, ο υπεύθυνος επεξεργασίας έχει και τις παρακάτω υποχρεώσεις και ο εργαζόμενος τα αντίστοιχα δικαιώματα :

Οφείλει να ενημερώσει τον εργαζόμενο εγγράφως

αα) για όλα τα παραπάνω στοιχεία (α-δ)

ββ) για τα δικαιώματά του, όπως αυτά αναλύονται εδώ.

γγ) με ποιες διατάξεις υποχρεούται (ο εργαζόμενος) να παράσχει τη συνδρομή του στην επεξεργασία των δεδομένων και τέλος,

δδ) για τις συνέπειες της άρνησής του, που τυχόν προβλέπονται ή από το νόμο ή από τη σύμβαση.

2. Το Δικαίωμα Πρόσβασης

Το δικαίωμα πρόσβασης, συναφές με το προηγούμενο δικαίωμα ενημέρωσης, συνίσταται στο δικαίωμα του εργαζόμενου να γνωρίζει

κάθε φορά το περιεχόμενο του προσωπικού του φακέλου, ποια δηλαδή από τα προσωπικά του δεδομένα αποτελούν ή αποτέλεσαν αντικείμενο επεξεργασίας. Το δικαίωμα αυτό περιλαμβάνει τις ακόλουθες πληροφορίες :

α) Όλα τα δεδομένα προσωπικού χαρακτήρα που τον αφορούν και την προέλευσή τους. Δικαιούται, δηλαδή, ο εργαζόμενος να πληροφορηθεί, όχι μόνο το περιεχόμενο, αλλά και τις πηγές από τις οποίες αντλήθηκαν οι πληροφορίες, π.χ. το γεγονός ότι ο εργαζόμενος ορισμένη ημέρα και ώρα, κατά την εκτέλεση της σύμβασης επιδείκνυε αμελή συμπεριφορά, συνέπεια της οποίας ήταν η ζημία του εργοδότη, πρέπει να συνοδεύεται και από την πηγή της πληροφορίας (βιντεοσκόπηση, άμεση γνώση εργοδότη ή αντιπροσώπού του κ.λπ.)

β) Τους σκοπούς της επεξεργασίας, τους αποδέκτες ή τις κατηγορίες των αποδεκτών.

γ) Την εξέλιξη της επεξεργασίας από την προηγούμενη ενημέρωση, ποια στοιχεία, δηλαδή, προστέθηκαν ή αφαιρέθηκαν στο φάκελο του εργαζόμενου και

δ) Τη λογική της αυτοματοποιημένης επεξεργασίας, δεδομένου ότι τα παραπάνω δικαιώματα είναι δυνατό να ασκηθούν και με τη συνδρομή ειδικού. Δεδομένα πάντως που αφορούν την υγεία, γνωστοποιούνται στο υποκείμενο μέσω γιατρού.

3. <u>Το Δικαίωμα Αντίρρησης</u>

Το δικαίωμα αντίρρησης συνίσταται στο δικαίωμα του εργαζόμενου να ζητήσει οποτεδήποτε, από τον υπεύθυνο επεξεργασίας, να προβεί σε συγκεκριμένη ενέργεια σχετικά με την επεξεργασία προσωπικών δεδομένων που τον αφορούν. Μπορεί, δηλαδή ο εργαζόμενος σχετικά με τα προσωπικά του δεδομένα να απευθύνει αίτηση με την οποία να ζητά συγκεκριμένη ενέργεια για όλα ή κάποια από τα προσωπικά του δεδομένα, των οποίων η επεξεργασία είναι παράνομη ή αντισυμβατική. Ενδεικτικά αναφέρονται στο νόμο τέτοιες περιπτώσεις, όπως η διόρθωση, προσωρινή μη χρησιμοποίηση, δέσμευση ή διαγραφή. Είναι αυτονόητο ότι στη σχέση εργασίας, προσωπικά δεδομένα απαιτούμενα ή από το νόμο ή από τη σύμβαση, τηρούνται νόμιμα και δεν είναι δυνατή η προβολή αντιρρήσεων περί αυτών, αφού αυτή θα ήταν παράνομη και

αντισυμβατική. Επομένως, το δικαίωμα αντίρρησης πρέπει να αφορά επεξεργασία πέραν των νομίμων ή συμβατικών σκοπών. Οι αντιρρήσεις του εργαζόμενου για να έχουν βάση πρέπει να επικαλούνται επεξεργασία που για οποιοδήποτε λόγο εξήλθε του παραπάνω αναφερόμενου πλαισίου, π.χ. ο εργαζόμενος έχει δικαίωμα να ζητήσει τη διαγραφή του αναφερόμενου περιστατικού της αμελούς συμπεριφοράς του, κατά τον χρόνο εκτέλεσης της σύμβασης, ως μη ανταποκρινόμενου στην αλήθεια, να ζητήσει τη διόρθωση της ηλικίας του, του χρόνου υπηρεσίας του στον ίδιο ή άλλο εργοδότη κ.λπ., τη διαγραφή δεδομένου υπερβαίνοντος το σκοπό του αρχείου, την προσωρινή μη χρησιμοποίηση δεδομένου, μέχρι να κριθεί αρμοδίως η βασιμότητά του ή τη μη διαβίβαση σε τρίτο, άσχετο με τις νόμιμες ή συμβατικές υποχρεώσεις.

Η άσκηση των παραπάνω δικαιωμάτων, πρόσβασης και αντίρρησης, γίνεται με αίτηση προς τον υπεύθυνο επεξεργασίας. Η αίτηση πρέπει περιέχει ορισμένο αίτημα για συγκεκριμένη ενέργεια (π.χ. αίτημα πρόσβασης, αίτημα διόρθωσης κ.λπ.).

Ο υπεύθυνος επεξεργασίας οφείλει να απαντήσει εντός 15 ημερών στον εργαζόμενο. Αν αυτό δεν συμβεί ή αν η απάντηση δεν κριθεί ικανοποιητική, ο εργαζόμενος δικαιούται να προσφύγει στην Αρχή, η οποία αφού εξετάσει στην ουσία το αίτημα εκδίδει οριστική απόφαση. Ο υπεύθυνος επεξεργασίας, άλλωστε, αν αρνηθεί να ικανοποιήσει το αίτημα, υποχρεούται να το γνωστοποιήσει στην Αρχή και στον εργαζόμενο, πληροφορώντας τον ότι δικαιούται να προσφύγει στην Αρχή. Αν το αίτημα γίνει δεκτό ο υπεύθυνος της επεξεργασίας υποχρεούται να χορηγήσει στον ενδιαφερόμενο σε γλώσσα κατανοητή αντίγραφο του διορθωμένου μέρους που τον αφορά.

4. <u>Δικαίωμα Δικαστικής Προστασίας</u>

Προσωρινή δικαστική προστασία (άρθρο 14)

Εκτός από τα παραπάνω δικαιώματα που έχει ο εργαζόμενος κατά την διαχείριση των προσωπικών του δεδομένων από τον εργοδότη, παρέχεται σ' αυτόν και το δικαίωμα προσωρινής δικαστικής προστασίας σε περίπτωση αυτοματοποιημένης επεξεργασίας των προσωπικών του δεδομένων, εφόσον αυτή αποβλέπει στην αξιολόγηση της

προσωπικότητάς του και ιδίως της αποδοτικότητάς του στην εργασία και της εν γένει συμπεριφοράς του. Όταν η επεξεργασία είναι αυτοματοποιημένη και αποβλέπει στους παραπάνω σκοπούς, ο εργαζόμενος έχει το δικαίωμα να προσφύγει στο αρμόδιο πολιτικό ή διοικητικό δικαστήριο και να ζητήσει την άμεση αναστολή ή μη εφαρμογή πράξης ή απόφασης που τον θίγει, ανεξάρτητα, αν συντρέχουν οι λοιπές προϋποθέσεις παροχής έννομης προστασίας. Είναι αυτονόητο ότι, όταν συντρέχουν οι προϋποθέσεις που προβλέπονται από διατάξεις ουσιαστικού ή δικονομικού δικαίου η προσωρινή προστασία δίδεται για οποιοδήποτε λόγο, αλλά και σε περίπτωση μη αυτοματοποιημένης εργασίας. Δικαίωμα οριστικής δικαστικής προστασίας δεν ορίζεται από το νόμο ως αυτονόητο.

5. <u>Αστική Ευθύνη (άρθρο 23)</u>

   Στο άρθρο 23 του ν.2472/1997 ρυθμίζεται ειδικώς το θέμα της αστικής ευθύνης του υπεύθυνου της επεξεργασίας έναντι του υποκειμένου των δεδομένων και επομένως και του εργαζόμενου. Διαλαμβάνεται δε ρητά ότι ο υπεύθυνος υποχρεούται να αποκαταστήσει πλήρως κάθε περιουσιακή βλάβη που προκάλεσε στον εργαζόμενο από την παράνομη επεξεργασία των προσωπικών του δεδομένων. Το ίδιο συμβαίνει και αν προκλήθηκε ηθική βλάβη την πιθανότητα επέλευσης της οποίας όφειλε να γνωρίζει ο υπόχρεος. Η χρηματική ικανοποίηση, λόγω ηθικής βλάβης, δεν μπορεί να είναι μικρότερη των δρχ. 200,000, εκτός αν ο ενάγων ζητήσει λιγότερα ή η παραβίαση οφείλεται σε αμέλεια.

   Στην §3 του άρθρου 23 ορίζεται τέλος ότι η εκδίκαση των σχετικών αγωγών γίνεται κατά την διαδικασία των άρθρων 664-676 ΚΠολΔ ότι η διαδικασία είναι άσχετη με την επέμβαση της Αρχής ή την άσκηση ποινικής δίωξης και ότι η απόφαση του Δικαστηρίου εκδίδεται μέσα σε δύο μήνες από την πρώτη συζήτηση στο ακροατήριο.

Η’ ΔΙΟΙΚΗΤΙΚΕΣ ΚΑΙ ΠΟΙΝΙΚΕΣ ΚΥΡΩΣΕΙΣ

Πρέπει εδώ να σημειωθεί ότι παραβάσεις του Νόμου για την προστασία των προσωπικών δεδομένων στον τομέα της εργασιακής σχέσης, συνεπάγονται διοικητικές κυρώσεις επιβαλλόμενες από την Αρχή,

όπως επίσης και ποινικές κυρώσεις προβλεπόμενες, επίσης από το Νόμο, ο οποίος δίδει ποινική απαξία και σε βαθμό κακουργήματος για παράνομη επεξεργασία δεδομένων προσωπικού χαρακτήρα. Οι διοικητικές κυρώσεις ορίζονται στο άρθρο 21του νόμου και είναι :

α) Η προειδοποίηση με αποκλειστική προθεσμία για άρση της παραβίασης.

β) Το πρόστιμο 300,000 –50,000,000 δρχ.

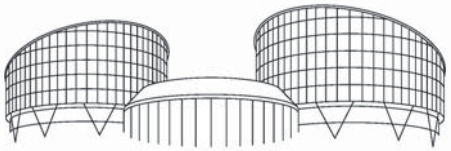
γ) Προσωρινή ανάκληση της άδειας και

ε) Καταστροφή του αρχείου ή διακοπή της επεξεργασίας και καταστροφή των σχετικών δεδομένων .

Οι ποινικές κυρώσεις αναφέρονται αναλυτικά στο άρθρο 22, αρχίζουν δε με φυλάκιση και χρηματική ποινή 1-5,000,000 δρχ. και καταλήγουν σε κάθειρξη (5-20 ετών) και χρηματική ποινή μέχρι δρχ.10,000,000

Ο Πρόεδρος **Η Γραμματέας**

Κωνσταντίνος Δαφέρμος **Ευγενία Τσιγγάνου**
Επιτ. Αντ/δρος Αρείου Πάγου



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

GRAND CHAMBER

CASE OF BĂRBULESCU v. ROMANIA

(Application no. 61496/08)

JUDGMENT

STRASBOURG

5 September 2017

This judgment is final but it may be subject to editorial revision.

In the case of Bărbulescu v. Romania,

The European Court of Human Rights, sitting as a Grand Chamber composed of:

Guido Raimondi, *President*,
Angelika Nußberger,
Mirjana Lazarova Trajkovska, *judges*,
Luis López Guerra, ad hoc *judge*,
Ledi Bianku,
Işıl Karakaş,
Nebojša Vučinić,
André Potocki,
Paul Lemmens,
Dmitry Dedov,
Jon Fridrik Kjølbro,
Mārtiņš Mits,
Armen Harutyunyan,
Stéphanie Mourou-Vikström,
Georges Ravarani,
Marko Bošnjak,
Tim Eicke, *judges*,

and Søren Prebensen, *Deputy Grand Chamber Registrar*,

Having deliberated in private on 30 November 2016 and on 8 June 2017,

Delivers the following judgment, which was adopted on the last-mentioned date:

PROCEDURE

1. The case originated in an application (no. 61496/08) against Romania lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Romanian national, Mr Bogdan Mihai Bărbulescu ("the applicant"), on 15 December 2008.

2. The applicant was represented by Mr E. Domokos-Hâncu and Mr O. Juverdeanu, lawyers practising in Bucharest. The Romanian Government ("the Government") were represented by their Agent, Ms C. Brumar, of the Ministry of Foreign Affairs.

3. The applicant complained, in particular, that his employer's decision to terminate his contract had been based on a breach of his right to respect for his private life and correspondence as enshrined in Article 8 of the Convention and that the domestic courts had failed to comply with their obligation to protect that right.

4. The application was allocated to the Fourth Section of the Court (Rule 52 § 1 of the Rules of Court). On 12 January 2016 a Chamber of that Section, composed of András Sajó, President, Vincent A. De Gaetano, Boštjan M. Zupančič, Nona Tsotsoria, Paulo Pinto de Albuquerque, Egidijus Kūris and Iulia Motoc, judges, and Fatoş Aracı, Deputy Section Registrar, unanimously declared the complaint concerning Article 8 of the Convention admissible and the remainder of the application inadmissible. It held, by six votes to one, that there had been no violation of Article 8 of the Convention. The dissenting opinion of Judge Pinto de Albuquerque was annexed to the Chamber judgment.

5. On 12 April 2016 the applicant requested the referral of the case to the Grand Chamber in accordance with Article 43 of the Convention and Rule 73. On 6 June 2016 a panel of the Grand Chamber accepted the request.

6. The composition of the Grand Chamber was determined in accordance with Article 26 §§ 4 and 5 of the Convention and Rule 24. Iulia Motoc, the judge elected in respect of Romania, withdrew from sitting in the case (Rule 28). Luis López Guerra was consequently appointed by the President to sit as an *ad hoc* judge (Article 26 § 4 of the Convention and Rule 29 § 1).

7. The applicant and the Government each filed further written observations (Rule 59 § 1).

8. In addition, third-party comments were received from the French Government and the European Trade Union Confederation, both having been given leave by the President to intervene in the written procedure (Article 36 § 2 of the Convention and Rule 44 § 3).

9. A hearing took place in public in the Human Rights Building, Strasbourg, on 30 November 2016 (Rule 59 § 3).

There appeared before the Court:

(a) *for the Government*
Ms C. BRUMAR, *Agent*,
Mr G.V. GAVRILĂ, member of the national legal service seconded to the Department of the Government Agent, *Counsel*,
Ms L.A. RUSU, Minister Plenipotentiary, Permanent Representation of Romania to the Council of Europe, *Adviser*;

(b) *for the applicant*
Mr E. DOMOKOS-HÂNCU,
Mr O. JUVERDEANU, *Counsel*.

The Court heard addresses by Mr Domokos-Hâncu, Mr Juverdeanu, Ms Brumar and Mr Gavrilă, and also their replies to questions from judges.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

10. The applicant was born in 1979 and lives in Bucharest.

11. From 1 August 2004 to 6 August 2007 he was employed in the Bucharest office of S., a Romanian private company ("the employer"), as a sales engineer. At his employer's request, for the purpose of responding to customers' enquiries, he created an instant messaging account using Yahoo Messenger, an online chat service offering real-time text transmission over the internet. He already had another personal Yahoo Messenger account.

12. The employer's internal regulations prohibited the use of company resources by employees in the following terms:

Article 50

"Any disturbance of order and discipline on company premises shall be strictly forbidden, in particular:

...

– ... personal use of computers, photocopiers, telephones or telex or fax machines."

13. The regulations did not contain any reference to the possibility for the employer to monitor employees' communications.

14. It appears from documents submitted by the Government that the applicant had been informed of the employer's internal regulations and had signed a copy of them on 20 December 2006 after acquainting himself with their contents.

15. On 3 July 2007 the Bucharest office received and circulated among all its employees an information notice that had been drawn up and sent by the Cluj head office on 26 June 2007. The employer asked employees to acquaint themselves with the notice and to sign a copy of it. The relevant parts of the notice read as follows:

"1. ... Time spent in the company must be quality time for everyone! Come to work to deal with company and professional matters, and not your own personal problems! Don't spend your time using the internet, the phone or the fax machine for matters unconnected to work or your duties. This is what [elementary education], common sense and the law dictate! The employer has a duty to supervise and monitor employees' work and to take punitive measures against anyone at fault!

Your misconduct will be carefully monitored and punished!

2. Because of repeated [disciplinary] offences *vis-à-vis* her superior, [as well as] her private use of the internet, the telephone and the photocopier, her negligence and her failure to perform her duties, Ms B.A. was dismissed on disciplinary grounds! Take a lesson from her bad example! Don't make the same mistakes!

3. Have a careful read of the collective labour agreement, the company's internal regulations, your job description and the employment contract you have signed! These are the basis of our collaboration! Between employer and employee! ..."

16. It also appears from the documents submitted by the Government, including the employer's attendance register, that the applicant acquainted himself with the notice and signed it between 3 and 13 July 2007.

17. In addition, it transpires that from 5 to 13 July 2007 the employer recorded the applicant's Yahoo Messenger communications in real time.

18. On 13 July 2007 at 4.30 p.m. the applicant was summoned by his employer to give an explanation. In the relevant notice he was informed that his Yahoo Messenger communications had been monitored and that there was evidence that he had used the internet for personal purposes, in breach of the internal regulations. Charts were attached indicating that his internet activity was greater than that of his colleagues. At that stage, he was not informed whether the monitoring of his communications had also concerned their content. The notice was worded as follows:

> "Please explain why you are using company resources (internet connection, Messenger) for personal purposes during working hours, as shown by the attached charts."

19. On the same day, the applicant informed the employer in writing that he had used Yahoo Messenger for work-related purposes only.

20. At 5.20 p.m. the employer again summoned him to give an explanation in a notice worded as follows:

> "Please explain why the entire correspondence you exchanged between 5 to 12 July 2007 using the S. Bucharest [internet] site ID had a private purpose, as shown by the attached forty-five pages."

21. The forty-five pages mentioned in the notice consisted of a transcript of the messages which the applicant had exchanged with his brother and his fiancée during the period when he had been monitored; the messages related to personal matters and some were of an intimate nature. The transcript also included five messages that the applicant had exchanged with his fiancée using his personal Yahoo Messenger account; these messages did not contain any intimate information.

22. Also on 13 July, the applicant informed the employer in writing that in his view it had committed a criminal offence, namely breaching the secrecy of correspondence.

23. On 1 August 2007 the employer terminated the applicant's contract of employment.

24. The applicant challenged his dismissal in an application to the Bucharest County Court ("the County Court"). He asked the court, firstly, to set aside the dismissal; secondly, to order his employer to pay him the amounts he was owed in respect of wages and any other entitlements and to reinstate him in his post; and thirdly, to order the employer to pay him 100,000 Romanian lei (approximately 30,000 euros) in damages for the harm resulting from the manner of his dismissal, and to reimburse his costs and expenses.

25. As to the merits, relying on *Copland v. the United Kingdom* (no. 62617/00, §§ 43-44, ECHR 2007-I), he argued that an employee's telephone and email communications from the workplace were covered by the notions of "private life" and "correspondence" and were therefore protected by Article 8 of the Convention. He also submitted that the decision to dismiss him was unlawful and that by monitoring his communications and accessing their contents his employer had infringed criminal law.

26. With regard specifically to the harm he claimed to have suffered, the applicant noted the manner of his dismissal and alleged that he had been subjected to harassment by his employer through the monitoring of his communications and the disclosure of their contents "to colleagues who were involved in one way or another in the dismissal procedure".

27. The applicant submitted evidence including a full copy of the transcript of his Yahoo Messenger communications and a copy of the information notice (see paragraph 15 above).

28. In a judgment of 7 December 2007 the County Court rejected the applicant's application and confirmed that his dismissal had been lawful. The relevant parts of the judgment read as follows:

> "The procedure for conducting a disciplinary investigation is expressly regulated by the provisions of Article 267 of the Labour Code.
>
> In the instant case it has been shown, through the written documents included in the file, that the employer conducted the disciplinary investigation in respect of the applicant by twice summoning him in writing to explain himself [and] specifying the subject, date, time and place of the interview, and that the applicant had the opportunity to submit arguments in his defence regarding his alleged acts, as is clear from the two explanatory notices included in the file (see copies on sheets 89 and 91).
>
> The court takes the view that the monitoring of the internet conversations in which the employee took part using the Yahoo Messenger software on the company's computer during working hours – regardless of whether or not the employer's actions were illegal in terms of criminal law – cannot undermine the validity of the disciplinary proceedings in the instant case.
>
> The fact that the provisions containing the requirement to interview the suspect (*învinuitul*) in a case of alleged misconduct and to examine the arguments submitted in that person's defence prior to the decision on a sanction are couched in imperative terms highlights the legislature's intention to make respect for the rights of the defence a prerequisite for the validity of the decision on the sanction.
>
> In the present case, since the employee maintained during the disciplinary investigation that he had not used Yahoo Messenger for personal purposes but in order to advise customers on the products being sold by his employer, the court takes the view that an inspection of the content of the [applicant's] conversations was the only way in which the employer could ascertain the validity of his arguments.
>
> The employer's right to monitor (*monitoriza*) employees in the workplace, [particularly] as regards their use of company computers, forms part of the broader right, governed by the provisions of Article 40 (d) of the Labour Code, to supervise how employees perform their professional tasks.

Given that it has been shown that the employees' attention had been drawn to the fact that, shortly before the applicant's disciplinary sanction, another employee had been dismissed for using the internet, the telephone and the photocopier for personal purposes, and that the employees had been warned that their activities were being monitored (see notice no. 2316 of 3 July 2007, which the applicant had signed [after] acquainting himself with it – see copy on sheet 64), the employer cannot be accused of showing a lack of transparency and of failing to give its employees a clear warning that it was monitoring their computer use.

Internet access in the workplace is above all a tool made available to employees by the employer for professional use, and the employer indisputably has the power, by virtue of its right to supervise its employees' activities, to monitor personal internet use.

Such checks by the employer are made necessary by, for example, the risk that through their internet use, employees might damage the company's IT systems, carry out illegal activities in cyberspace for which the company could incur liability, or disclose the company's trade secrets.

The court considers that the acts committed by the applicant constitute a disciplinary offence within the meaning of Article 263 § 2 of the Labour Code since they amount to a culpable breach of the provisions of Article 50 of S.'s internal regulations ..., which prohibit the use of computers for personal purposes.

The aforementioned acts are deemed by the internal regulations to constitute serious misconduct, the penalty for which, in accordance with Article 73 of the same internal regulations, [is] termination of the contract of employment on disciplinary grounds.

Having regard to the factual and legal arguments set out above, the court considers that the decision complained of is well-founded and lawful, and dismisses the application as unfounded."

29. The applicant appealed to the Bucharest Court of Appeal ("the Court of Appeal"). He repeated the arguments he had submitted before the first-instance court and contended in addition that that court had not struck a fair balance between the interests at stake, unjustly prioritising the employer's interest in enjoying discretion to control its employees' time and resources. He further argued that neither the internal regulations nor the information notice had contained any indication that the employer could monitor employees' communications.

30. The Court of Appeal dismissed the applicant's appeal in a judgment of 17 June 2008, the relevant parts of which read:

"The first-instance court has rightly concluded that the internet is a tool made available to employees by the employer for professional use, and that the employer is entitled to set rules for the use of this tool, by laying down prohibitions and provisions which employees must observe when using the internet in the workplace; it is clear that personal use may be refused, and the employees in the present case were duly informed of this in a notice issued on 26 June 2007 in accordance with the provisions of the internal regulations, in which they were instructed to observe working hours, to be present at the workplace [during those hours and] to make effective use of working time.

In conclusion, an employer who has made an investment is entitled, in exercising the rights enshrined in Article 40 § 1 of the Labour Code, to monitor internet use in

the workplace, and an employee who breaches the employer's rules on personal internet use is committing a disciplinary offence that may give rise to a sanction, including the most serious one.

There is undoubtedly a conflict between the employer's right to engage in monitoring and the employees' right to protection of their privacy. This conflict has been settled at European Union level through the adoption of Directive no. 95/46/EC, which has laid down a number of principles governing the monitoring of internet and email use in the workplace, including the following in particular.

- Principle of necessity: monitoring must be necessary to achieve a certain aim.

- Principle of purpose specification: data must be collected for specified, explicit and legitimate purposes.

- Principle of transparency: the employer must provide employees with full information about monitoring operations.

- Principle of legitimacy: data-processing operations may only take place for a legitimate purpose.

- Principle of proportionality: personal data being monitored must be relevant and adequate in relation to the specified purpose.

- Principle of security: the employer is required to take all possible security measures to ensure that the data collected are not accessible to third parties.

In view of the fact that the employer has the right and the duty to ensure the smooth running of the company and, to that end, [is entitled] to supervise how its employees perform their professional tasks, and the fact [that it] enjoys disciplinary powers which it may legitimately use and which [authorised it in the present case] to monitor and transcribe the communications on Yahoo Messenger which the employee denied having exchanged for personal purposes, after he and his colleagues had been warned that company resources should not be used for such purposes, it cannot be maintained that this legitimate aim could have been achieved by any other means than by breaching the secrecy of his correspondence, or that a fair balance was not struck between the need to protect [the employee's] privacy and the employer's right to supervise the operation of its business.

...

Accordingly, having regard to the considerations set out above, the court finds that the decision of the first-instance court is lawful and well-founded and that the appeal is unfounded; it must therefore be dismissed, in accordance with the provisions of Article 312 § 1 of the C[ode of] Civ[il] Pr[ocedure]."

31. In the meantime, on 18 September 2007 the applicant had lodged a criminal complaint against the statutory representatives of S., alleging a breach of the secrecy of correspondence. On 9 May 2012 the Directorate for Investigating Organised Crime and Terrorism (DIICOT) of the prosecutor's office attached to the Supreme Court of Cassation and Justice ruled that there was no case to answer, on the grounds that the company was the owner of the computer system and the internet connection and could therefore monitor its employees' internet activity and use the information stored on the server, and in view of the prohibition on personal use of the IT systems, as a result of which the monitoring had been foreseeable. The

applicant did not avail himself of the opportunity provided for by the applicable procedural rules to challenge the prosecuting authorities' decision in the domestic courts.

II. RELEVANT DOMESTIC LAW

A. The Constitution

32. The relevant parts of the Romanian Constitution provide:

Article 26

"1. The public authorities shall respect and protect intimate, family and private life."

Article 28

"The secrecy of letters, telegrams, other postal communications, telephone conversations and any other lawful means of communication is inviolable."

B. The Criminal Code

33. The relevant parts of the Criminal Code as in force at the material time read as follows:

Article 195 – Breach of secrecy of correspondence

"1. Anyone who unlawfully opens somebody else's correspondence or intercepts somebody else's conversations or communication by telephone, by telegraph or by any other long-distance means of transmission shall be liable to imprisonment for between six months and three years."

C. The Civil Code

34. The relevant provisions of the Civil Code as in force at the time of the events were worded as follows:

Article 998

"Any act committed by a person that causes damage to another shall render the person through whose fault the damage was caused liable to make reparation for it."

Article 999

"Everyone shall be liable for damage he has caused not only through his own acts but also through his failure to act or his negligence."

D. The Labour Code

35. As worded at the material time, the Labour Code provided:

Article 40

"1. The employer shall in principle have the following rights:

...

(d) to supervise how [employees] perform their professional tasks;

...

2. The employer shall in principle have the following duties:

...

(i) to guarantee the confidentiality of employees' personal data."

E. Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

36. The relevant parts of Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Law no. 677/2001"), which reproduces certain provisions of Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (see paragraph 45 below), provide:

Article 3 – Definitions

"For the purposes of this Law:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

..."

Article 5 – Conditions for the legitimacy of data processing

"1. Personal data ... may not be processed in any way unless the data subject has explicitly and unambiguously consented to it.

2. The consent of the data subject shall not be necessary in the following circumstances:

(a) where processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

...

(e) where processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject;

...

3. The provisions of paragraph 2 are without prejudice to the statutory provisions governing the public authorities' duty to respect and protect intimate, family and private life."

Article 18 – Right to apply to the courts

"1. Data subjects shall be entitled, without prejudice to the possibility of lodging a complaint with the supervisory authority, to apply to the courts for protection of the rights safeguarded by this Act that have been infringed.

2. Any person who has suffered damage as a result of the unlawful processing of his or her personal data may apply to the competent court for compensation [for the damage].

..."

III. INTERNATIONAL LAW AND PRACTICE

A. United Nations standards

37. The Guidelines for the regulation of computerized personal data files, adopted by the United Nations General Assembly on 14 December 1990 in Resolution 45/95 (A/RES/45/95), lay down the minimum guarantees that should be provided for in national legislation. The relevant principles read as follows:

"**1. Principle of lawfulness and fairness**

Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the United Nations.

2. Principle of accuracy

Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

3. Principle of purpose specification

The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

(a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified;

(b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;

(c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purposes so specified.

4. Principle of interested-person access

Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful, unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8 below. The cost of any rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

...

6. Power to make exceptions

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, *inter alia*, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

..."

38. The International Labour Office (ILO) issued a Code of Practice on the Protection of Workers' Personal Data ("the ILO Code of Practice") in 1997, laying down the following principles:

"**5. General principles**

5.1. Personal data should be processed lawfully and fairly, and only for reasons directly relevant to the employment of the worker.

5.2. Personal data should, in principle, be used only for the purposes for which they were originally collected.

5.3. If personal data are to be processed for purposes other than those for which they were collected, the employer should ensure that they are not used in a manner incompatible with the original purpose, and should take the necessary measures to avoid any misinterpretations caused by a change of context.

5.4. Personal data collected in connection with technical or organizational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers.

5.5. Decisions concerning a worker should not be based solely on the automated processing of that worker's personal data.

5.6. Personal data collected by electronic monitoring should not be the only factors in evaluating worker performance.

5.7. Employers should regularly assess their data processing practices:

(a) to reduce as far as possible the kind and amount of personal data collected; and

(b) to improve ways of protecting the privacy of workers.

5.8. Workers and their representatives should be kept informed of any data collection process, the rules that govern that process, and their rights.

...

5.13. Workers may not waive their privacy rights."

39. With regard to the more specific issue of monitoring of workers, the ILO Code of Practice states as follows:

"**6. Collection of personal data**

6.1. All personal data should, in principle, be obtained from the individual worker.

...

6.14. (1) If workers are monitored they should be informed in advance of the reasons for monitoring, the time schedule, the methods and techniques used and the data to be collected, and the employer must minimize the intrusion on the privacy of workers.

(2) Secret monitoring should be permitted only:

(a) if it is in conformity with national legislation; or

(b) if there is suspicion on reasonable grounds of criminal activity or other serious wrongdoing.

(3) Continuous monitoring should be permitted only if required for health and safety or the protection of property."

40. The ILO Code of Practice also includes an inventory of workers' individual rights, particularly as regards information about the processing of personal data, access to such data and reviews of any measures taken. The relevant parts read as follows:

"**11. Individual rights**

11.1. Workers should have the right to be regularly notified of the personal data held about them and the processing of that personal data.

11.2. Workers should have access to all their personal data, irrespective of whether the personal data are processed by automated systems or are kept in a particular manual file regarding the individual worker or in any other file which includes workers' personal data.

11.3. The workers' right to know about the processing of their personal data should include the right to examine and obtain a copy of any records to the extent that the data contained in the record includes that worker's personal data.

...

11.8. Employers should, in the event of a security investigation, have the right to deny the worker access to that worker's personal data until the close of the investigation and to the extent that the purposes of the investigation would be

threatened. No decision concerning the employment relationship should be taken, however, before the worker has had access to all the worker's personal data.

11.9. Workers should have the right to demand that incorrect or incomplete personal data, and personal data processed inconsistently with the provisions of this code, be deleted or rectified.

...

11.13. In any legislation, regulation, collective agreement, work rules or policy developed consistent with the provisions of this code, there should be specified an avenue of redress for workers to challenge the employer's compliance with the instrument. Procedures should be established to receive and respond to any complaint lodged by workers. The complaint process should be easily accessible to workers and be simple to use."

41. In addition, on 18 December 2013 the United Nations General Assembly adopted Resolution no. 68/167 on the right to privacy in the digital age (A/RES/68/167), in which, *inter alia*, it called upon States:

"(*a*) To respect and protect the right to privacy, including in the context of digital communication;

(*b*) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law;

(*c*) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(*d*) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data[.]"

B. Council of Europe standards

42. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981, ETS no. 108), which came into force in respect of Romania on 1 June 2002, includes the following provisions in particular:

Article 2 – Definitions

"For the purposes of this Convention:

(a) 'personal data' means any information relating to an identified or identifiable individual ('data subject');

...

(c) 'automatic processing' includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or

arithmetical operations on those data, their alteration, erasure, retrieval or dissemination;

...”

Article 3 – Scope

“1. The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors.

...”

Article 5 – Quality of data

“Personal data undergoing automatic processing shall be:

(a) obtained and processed fairly and lawfully;

(b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

(d) accurate and, where necessary, kept up to date;

(e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.”

Article 8 – Additional safeguards for the data subject

“Any person shall be enabled:

(a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

(b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

...

(d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.”

Article 9 – Exceptions and restrictions

“...

2. Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

(a) protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

(b) protecting the data subject or the rights and freedoms of others;

...”

Article 10 – Sanctions and remedies

"Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter."

43. Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, which was adopted on 1 April 2015, states in particular:

"**4. Application of data processing principles**

4.1. Employers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned.

...

6. Internal use of data

6.1. Personal data collected for employment purposes should only be processed by employers for such purposes.

6.2. Employers should adopt data protection policies, rules and/or other instruments on internal use of personal data in compliance with the principles of the present recommendation.

...

10. Transparency of processing

10.1. Information concerning personal data held by employers should be made available either to the employee concerned directly or through the intermediary of his or her representatives, or brought to his or her notice through other appropriate means.

10.2. Employers should provide employees with the following information:

– the categories of personal data to be processed and a description of the purposes of the processing;

– the recipients, or categories of recipients of the personal data;

– the means employees have of exercising the rights set out in principle 11 of the present recommendation, without prejudice to more favourable ones provided by domestic law or in their legal system;

– any other information necessary to ensure fair and lawful processing.

10.3. A particularly clear and complete description must be provided of the categories of personal data that can be collected by ICTs, including video surveillance and their possible use. This principle also applies to the particular forms of processing provided for in Part II of the appendix to the present recommendation.

10.4. The information should be provided in an accessible format and kept up to date. In any event, such information should be provided before an employee carries out the activity or action concerned, and made readily available through the information systems normally used by the employee.

...

14. Use of Internet and electronic communications in the workplace

14.1. Employers should avoid unjustifiable and unreasonable interferences with employees' right to private life. This principle extends to all technical devices and ICTs used by an employee. The persons concerned should be properly and periodically informed in application of a clear privacy policy, in accordance with principle 10 of the present recommendation. The information provided should be kept up to date and should include the purpose of the processing, the preservation or back-up period of traffic data and the archiving of professional electronic communications.

14.2. In particular, in the event of processing of personal data relating to Internet or Intranet pages accessed by the employee, preference should be given to the adoption of preventive measures, such as the use of filters which prevent particular operations, and to the grading of possible monitoring on personal data, giving preference for non-individual random checks on data which are anonymous or in some way aggregated.

14.3. Access by employers to the professional electronic communications of their employees who have been informed in advance of the existence of that possibility can only occur, where necessary, for security or other legitimate reasons. In case of absent employees, employers should take the necessary measures and foresee the appropriate procedures aimed at enabling access to professional electronic communications only when such access is of professional necessity. Access should be undertaken in the least intrusive way possible and only after having informed the employees concerned.

14.4. The content, sending and receiving of private electronic communications at work should not be monitored under any circumstances.

14.5. On an employee's departure from an organisation, the employer should take the necessary organisational and technical measures to automatically deactivate the employee's electronic messaging account. If employers need to recover the contents of an employee's account for the efficient running of the organisation, they should do so before his or her departure and, when feasible, in his or her presence."

IV. EUROPEAN UNION LAW

44. The relevant provisions of the Charter of Fundamental Rights of the European Union (2007/C 303/01) are worded as follows:

Article 7 – Respect for private and family life

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 8 – Protection of personal data

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

45. Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals

with regard to the processing of personal data and on the free movement of such data ("Directive 95/46/EC") states that the object of national laws on the processing of personal data is notably to protect the right to privacy, as recognised both in Article 8 of the Convention and in the general principles of Community law. The relevant provisions of Directive 95/46/EC read as follows:

Article 2 – Definitions

"For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

..."

Article 6

"1. Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes . Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

2. It shall be for the controller to ensure that paragraph 1 is complied with."

Article 7

"Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).”

Article 8 – The processing of special categories of data

“1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject’s giving his consent; or

(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or

...

(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

...

4. Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority.”

46. A Working Party on Data Protection (“the Working Party”) has been set up under Article 29 of the Directive and, in accordance with Article 30, is empowered to:

“(a) examine any question covering the application of the national measures adopted under this Directive in order to contribute to the uniform application of such measures;

(b) give the Commission an opinion on the level of protection in the Community and in third countries;

(c) advise the Commission on any proposed amendment of this Directive, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data and on any other proposed Community measures affecting such rights and freedoms;

(d) give an opinion on codes of conduct drawn up at Community level.”

The Working Party is an independent advisory body of the European Union. It issued an opinion in September 2001 on the processing of personal data in an employment context (opinion 8/2001), which summarises the fundamental data-protection principles: finality, transparency, legitimacy, proportionality, accuracy, security and staff awareness. In the opinion, which it adopted in conformity with its role of contributing to the uniform application of national measures adopted under Directive 95/46/EC, the Working Party pointed out that the monitoring of email involved the processing of personal data, and expressed the view that any monitoring of employees had to be

> "a proportionate response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers."

47. In May 2002 the Working Party produced a working document on surveillance and monitoring of electronic communications in the workplace ("the working document"), in which it expressly took into account the provisions of Directive 95/46/EC read in the light of the provisions of Article 8 of the Convention. The working document asserts that the simple fact that a monitoring activity or surveillance is considered convenient to serve an employer's interest cannot in itself justify an intrusion into workers' privacy, and that any monitoring measure must satisfy four criteria: transparency, necessity, fairness and proportionality.

48. Regarding the technical aspect, the working document states:

> "Prompt information can be easily delivered by software such as warning windows, which pop up and alert the worker that the system has detected and/or has taken steps to prevent an unauthorised use of the network."

49. More specifically, with regard to the question of access to employees' emails, the working document includes the following passage:

> "It would only be in exceptional circumstances that the monitoring of a worker's [e]mail or Internet use would be considered necessary. For instance, monitoring of a worker's email may become necessary in order to obtain confirmation or proof of certain actions on his part. Such actions would include criminal activity on the part of the worker insofar as it is necessary for the employer to defend his own interests, for example, where he is vicariously liable for the actions of the worker. These activities would also include detection of viruses and in general terms any activity carried out by the employer to guarantee the security of the system.
>
> It should be mentioned that opening an employee's email may also be necessary for reasons other than monitoring or surveillance, for example in order to maintain correspondence in case the employee is out of office (e.g. due to sickness or leave) and correspondence cannot be guaranteed otherwise (e.g. via auto reply or automatic forwarding)."

50. The Court of Justice of the European Union has interpreted the provisions of Directive 95/46/EC in the light of the right to respect for private life, as guaranteed by Article 8 of the Convention, in the case of

Österreichischer Rundfunk and Others (C-465/00, C-138/01 and C-139/01, judgment of 20 May 2003, ECLI:EU:C:2003:294, paragraphs 71 et seq.).

51. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), published in OJ 2016 L 119/1, entered into force on 24 May 2016 and will repeal Directive 95/46/EC with effect from 25 May 2018 (Article 99). The relevant provisions of the Regulation read as follows:

Article 30 – Records of processing activities

"1 Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

(a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of the processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

(a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

(b) the categories of processing carried out on behalf of each controller;

(c) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;

(d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10."

Article 47 – Binding corporate rules

"1. The competent supervisory authority shall approve binding corporate rules in accordance with the consistency mechanism set out in Article 63, provided that they:

(a) are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

(b) expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

(c) fulfil the requirements laid down in paragraph 2.

2. The binding corporate rules referred to in paragraph 1 shall specify at least:

(a) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

(b) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

(c) their legally binding nature, both internally and externally;

(d) the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

(e) the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling in accordance with Article 22, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with Article 79, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

(f) the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

(g) how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to Articles 13 and 14;

(h) the tasks of any data protection officer designated in accordance with Article 37 or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

(i) the complaint procedures;

(j) the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

(k) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

(l) the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

(m) the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

(n) the appropriate data protection training to personnel having permanent or regular access to personal data.

3. The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Article. Those implementing acts shall be adopted in accordance with the examination procedure set out in Article 93(2).”

Article 88 – Processing in the context of employment

“1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer’s or customer’s property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject’s human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group

of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place.

3. Each Member State shall notify to the Commission those provisions of its law which it adopts pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them."

V. COMPARATIVE LAW

52. The documents available to the Court concerning the legislation of the Council of Europe member States, in particular a study of thirty-four of them, indicate that all the States concerned recognise in general terms, at constitutional or statutory level, the right to privacy and to secrecy of correspondence. However, only Austria, Finland, Luxembourg, Portugal, Slovakia and the United Kingdom have explicitly regulated the issue of workplace privacy, whether in labour laws or in special legislation.

53. With regard to monitoring powers, thirty-four Council of Europe member States require employers to give employees prior notice of monitoring. This may take a number of forms, for example notification of the personal data-protection authorities or of workers' representatives. The existing legislation in Austria, Estonia, Finland, Greece, Lithuania, Luxembourg, Norway, Poland, Slovakia and the former Yugoslav Republic of Macedonia requires employers to notify employees directly before initiating the monitoring.

54. In, Austria, Denmark, Finland, France, Germany, Greece, Italy, Portugal and Sweden, employers may monitor emails marked by employees as "private", without being permitted to access their content. In Luxembourg employers may not open emails that are either marked as "private" or are manifestly of a private nature. The Czech Republic, Italy and Slovenia, as well as the Republic of Moldova to a certain extent, also limit the extent to which employers may monitor their employees' communications, according to whether the communications are professional or personal in nature. In Germany and Portugal, once it has been established that a message is private, the employer must stop reading it.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

55. The applicant submitted that his dismissal by his employer had been based on a breach of his right to respect for his private life and correspondence and that, by not revoking that measure, the domestic courts

had failed to comply with their obligation to protect the right in question. He relied on Article 8 of the Convention, which provides:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A. The Chamber's findings

56. In its judgment of 12 January 2016 the Chamber held, firstly, that Article 8 of the Convention was applicable in the present case. Referring to the concept of reasonable expectation of privacy, it found that the present case differed from *Copland* (cited above, § 41) and *Halford v. the United Kingdom* (25 June 1997, § 45, *Reports of Judgments and Decisions* 1997-III) in that the applicant's employer's internal regulations in the present case strictly prohibited employees from using company computers and resources for personal purposes. The Chamber had regard to the nature of the applicant's communications and the fact that a transcript of them had been used as evidence in the domestic court proceedings, and concluded that the applicant's right to respect for his "private life" and "correspondence" was at stake.

57. Next, the Chamber examined the case from the standpoint of the State's positive obligations, since the decision to dismiss the applicant had been taken by a private-law entity. It therefore determined whether the national authorities had struck a fair balance between the applicant's right to respect for his private life and correspondence and his employer's interests.

58. The Chamber noted that the applicant had been able to bring his case and raise his arguments before the labour courts. The courts had found that he had committed a disciplinary offence by using the internet for personal purposes during working hours, and to that end they had had regard to the conduct of the disciplinary proceedings, in particular the fact that the employer had accessed the contents of the applicant's communications only after the applicant had declared that he had used Yahoo Messenger for work-related purposes.

59. The Chamber further noted that the domestic courts had not based their decisions on the contents of the applicant's communications and that the employer's monitoring activities had been limited to his use of Yahoo Messenger.

60. Accordingly, it held that there had been no violation of Article 8 of the Convention.

B. Scope of the case before the Grand Chamber

61. The Court notes that in the proceedings before the Chamber the applicant alleged that his employer's decision to terminate his contract had been based on a breach of his right to respect for his private life and correspondence as enshrined in Article 8 of the Convention and that, by not revoking that measure, the domestic courts had failed to comply with their obligation to protect the right in question. The Chamber declared this complaint admissible on 12 January 2016.

62. The Court reiterates that the case referred to the Grand Chamber is the application as it has been declared admissible by the Chamber (see *K. and T. v. Finland* [GC], no. 25702/94, §§ 140-41, ECHR 2001-VII; *D.H. and Others v. the Czech Republic* [GC], no. 57325/00, § 109, ECHR 2007-IV; and *Blokhin v. Russia* [GC], no. 47152/06, § 91, ECHR 2016).

63. In his observations before the Grand Chamber, the applicant complained for the first time about the rejection in 2012 of the criminal complaint filed by him in connection with an alleged breach of the secrecy of correspondence (see paragraph 90 below).

64. This new complaint was not mentioned in the decision of 12 January 2016 as to admissibility, which defines the boundaries of the examination of the application. It therefore falls outside the scope of the case as referred to the Grand Chamber, which accordingly does not have jurisdiction to deal with it and will limit its examination to the complaint that was declared admissible by the Chamber.

C. Applicability of Article 8 of the Convention

1. The parties' submissions

(a) The Government

65. The Government argued that the applicant could not claim any expectation of "privacy" as regards the communications he had exchanged via an instant messaging account created for professional use. With reference to the case-law of the French and Cypriot courts, they submitted that messages sent by an employee using the technical facilities made available to him by his employer had to be regarded as professional in nature unless the employee explicitly identified them as private. They noted that it was not technically possible using Yahoo Messenger to mark messages as private; nevertheless, the applicant had had an adequate opportunity, during the initial stage of the disciplinary proceedings, to indicate that his communications had been private, and yet had chosen to maintain that they had been work-related. The applicant had been informed not only of his employer's internal regulations, which prohibited all

personal use of company resources, but also of the fact that his employer had initiated a process for monitoring his communications.

66. The Government relied on three further arguments in contending that Article 8 of the Convention was not applicable in the present case. Firstly, there was no evidence to suggest that the transcript of the applicant's communications had been disclosed to his work colleagues; the applicant himself had produced the full transcript of the messages in the proceedings before the domestic courts, without asking for any restrictions to be placed on access to the documents concerned. Secondly, the national authorities had used the transcript of the messages as evidence because the applicant had so requested, and because the prosecuting authorities had already found that the monitoring of his communications had been lawful. Thirdly, the information notice had contained sufficient indications for the applicant to have been aware that his employer could monitor his communications, and this had rendered them devoid of any private element.

(b) The applicant

67. The applicant did not make any submissions as to the applicability of Article 8 of the Convention, but repeatedly maintained that his communications had been private in nature.

68. He further argued that, since he had created the Yahoo Messenger account in question and was the only person who knew the password, he had had a reasonable expectation of privacy regarding his communications. He also asserted that he had not received prior notification from his employer about the monitoring of his communications.

2. The Court's assessment

69. The Court notes that the question arising in the present case is whether the matters complained of by the applicant fall within the scope of Article 8 of the Convention.

70. At this stage of its examination it considers it useful to emphasise that "private life" is a broad term not susceptible to exhaustive definition (see *Sidabras and Džiautas v. Lithuania*, nos. 55480/00 and 59330/00, § 43, ECHR 2004-VIII). Article 8 of the Convention protects the right to personal development (see *K.A. and A.D. v. Belgium*, nos. 42758/98 and 45558/99, § 83, 17 February 2005), whether in terms of personality (see *Christine Goodwin v. the United Kingdom* [GC], no. 28957/95, § 90, ECHR 2002-VI) or of personal autonomy, which is an important principle underlying the interpretation of the Article 8 guarantees (see *Pretty v. the United Kingdom*, no. 2346/02, § 61, ECHR 2002-III). The Court acknowledges that everyone has the right to live privately, away from unwanted attention (see *Smirnova v. Russia*, nos. 46133/99 and 48183/99, § 95, ECHR 2003-IX (extracts)). It also considers that it would be too restrictive to limit the notion of "private life" to an "inner circle" in which the individual may live his or her own

personal life as he or she chooses, thus excluding entirely the outside world not encompassed within that circle (see *Niemietz v. Germany*, 16 December 1992, § 29, Series A no. 251-B). Article 8 thus guarantees a right to "private life" in the broad sense, including the right to lead a "private social life", that is, the possibility for the individual to develop his or her social identity. In that respect, the right in question enshrines the possibility of approaching others in order to establish and develop relationships with them (see *Bigaeva v. Greece*, no. 26713/05, § 22, 28 May 2009, and *Özpınar v. Turkey*, no. 20999/04, § 45 *in fine*, 19 October 2010).

71. The Court considers that the notion of "private life" may include professional activities (see *Fernández Martínez v. Spain* [GC], no. 56030/07, § 110, ECHR 2014 (extracts), and *Oleksandr Volkov v. Ukraine*, no. 21722/11, §§ 165-66, ECHR 2013), or activities taking place in a public context (see *Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, § 95, ECHR 2012). Restrictions on an individual's professional life may fall within Article 8 where they have repercussions on the manner in which he or she constructs his or her social identity by developing relationships with others. It should be noted in this connection that it is in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity to develop relationships with the outside world (see *Niemietz*, cited above, § 29).

72. Furthermore, as regards the notion of "correspondence", it should be noted that in the wording of Article 8 this word is not qualified by any adjective, unlike the term "life". And indeed, the Court has already held that, in the context of correspondence by means of telephone calls, no such qualification is to be made. In a number of cases relating to correspondence with a lawyer, it has not even envisaged the possibility that Article 8 might be inapplicable on the ground that the correspondence was of a professional nature (see *Niemietz*, cited above, § 32, with further references). Furthermore, it has held that telephone conversations are covered by the notions of "private life" and "correspondence" within the meaning of Article 8 (see *Roman Zakharov v. Russia* [GC], no. 47143/06, § 173, ECHR 2015). In principle, this is also true where telephone calls are made from or received on business premises (see *Halford*, cited above, § 44, and *Amann v. Switzerland* [GC], no. 27798/95, § 44, ECHR 2000-II). The same applies to emails sent from the workplace, which enjoy similar protection under Article 8, as does information derived from the monitoring of a person's internet use (see *Copland*, cited above, § 41 *in fine*).

73. It is clear from the Court's case-law that communications from business premises as well as from the home may be covered by the notions of "private life" and "correspondence" within the meaning of Article 8 of the Convention (see *Halford*, cited above, § 44; and *Copland*, cited above, § 41). In order to ascertain whether the notions of "private life" and "correspondence" are applicable, the Court has on several occasions

examined whether individuals had a reasonable expectation that their privacy would be respected and protected (ibid.; and as regards "private life", see also *Köpke v. Germany* (dec.), no. 420/07, 5 October 2010). In that context, it has stated that a reasonable expectation of privacy is a significant though not necessarily conclusive factor (see *Köpke*, cited above).

74. Applying these principles in the present case, the Court first observes that the kind of internet instant messaging service at issue is just one of the forms of communication enabling individuals to lead a private social life. At the same time, the sending and receiving of communications is covered by the notion of "correspondence", even if they are sent from an employer's computer. The Court notes, however, that the applicant's employer instructed him and the other employees to refrain from any personal activities in the workplace. This requirement on the employer's part was reflected in measures including a ban on using company resources for personal purposes (see paragraph 12 above).

75. The Court further notes that with a view to ensuring that this requirement was met, the employer set up a system for monitoring its employees' internet use (see paragraphs 17 and 18 above). The documents in the case file, in particular those relating to the disciplinary proceedings against the applicant, indicate that during the monitoring process, both the flow and the content of the applicants' communications were recorded and stored (see paragraphs 18 and 20 above).

76. The Court observes in addition that despite this requirement on the employer's part, the applicant exchanged messages of a personal nature with his fiancée and his brother (see paragraph 21 above). Some of these messages were of an intimate nature (ibid.).

77. The Court considers that it is clear from the case file that the applicant had indeed been informed of the ban on personal internet use laid down in his employer's internal regulations (see paragraph 14 above). However, it is not so clear that he had been informed prior to the monitoring of his communications that such a monitoring operation was to take place. Thus, the Government submitted that the applicant had acquainted himself with the employer's information notice on an unspecified date between 3 and 13 July 2007 (see paragraph 16 above). Nevertheless, the domestic courts omitted to ascertain whether the applicant had been informed of the monitoring operation before the date on which it began, given that the employer recorded communications in real time from 5 to 13 July 2007 (see paragraph 17 above).

78. In any event, it does not appear that the applicant was informed in advance of the extent and nature of his employer's monitoring activities, or of the possibility that the employer might have access to the actual contents of his communications.

79. The Court also takes note of the applicant's argument that he himself had created the Yahoo Messenger account in question and was the only

person who knew the password (see paragraph 68 above). In addition, it observes that the material in the case file indicates that the employer also accessed the applicant's personal Yahoo Messenger account (see paragraph 21 above). Be that as it may, the applicant had created the Yahoo Messenger account in issue on his employer's instructions to answer customers' enquiries (see paragraph 11 above), and the employer had access to it.

80. It is open to question whether – and if so, to what extent – the employer's restrictive regulations left the applicant with a reasonable expectation of privacy. Be that as it may, an employer's instructions cannot reduce private social life in the workplace to zero. Respect for private life and for the privacy of correspondence continues to exist, even if these may be restricted in so far as necessary.

81. In the light of all the above considerations, the Court concludes that the applicant's communications in the workplace were covered by the concepts of "private life" and "correspondence". Accordingly, in the circumstances of the present case, Article 8 of the Convention is applicable.

D. Compliance with Article 8 of the Convention

1. The parties' submissions and third-party comments

(a) The applicant

82. In his written observations before the Grand Chamber, the applicant submitted that the Chamber had not taken sufficient account of certain factual aspects of the case. Firstly, he emphasised the specific features of Yahoo Messenger, which was designed for personal use. His employer's decision to use this tool in a work context did not alter the fact that it was essentially intended to be used for personal purposes. He thus considered himself to be the sole owner of the Yahoo Messenger account that he had opened at his employer's request.

83. Secondly, the applicant argued that his employer had not introduced any policy on internet use. He had not had any warning of the possibility that his communications might be monitored or read; nor had he given any consent in that regard. If such a policy had been in place and he had been informed of it, he would have refrained from disclosing certain aspects of his private life on Yahoo Messenger.

84. Thirdly, the applicant contended that a distinction should be drawn between personal internet use having a profit-making purpose and "a small harmless private conversation" which had not sought to derive any profit and had not caused any damage to his employer; he pointed out in that connection that during the disciplinary proceedings against him, the employer had not accused him of having caused any damage to the company. The applicant highlighted developments in information and communication technologies, as well as in the social customs and habits

linked to their use. He submitted that contemporary working conditions made it impossible to draw a clear dividing line between private and professional life, and disputed the legitimacy of any management policy prohibiting personal use of the internet and of any connected devices.

85. From a legal standpoint, the applicant submitted that the Romanian State had not fulfilled its positive obligations under Article 8 of the Convention. More specifically, the domestic courts had not overturned his dismissal despite having acknowledged that there had been a violation of his right to respect for his private communications.

86. Firstly, he submitted that the Chamber had incorrectly distinguished the present case from *Copland* (cited above, § 42). In his view, the decisive factor in analysing the case was not whether the employer had tolerated personal internet use, but the fact that the employer had not warned the employee that his communications could be monitored. In that connection, he contended that his employer had first placed him under surveillance and had only afterwards given him the opportunity to specify whether his communications were private or work-related. The Court had to examine both whether an outright ban on personal internet use entitled the employer to monitor its employees, and whether the employer had to give reasons for such monitoring.

87. Secondly, the applicant submitted that the Chamber's analysis in relation to the second paragraph of Article 8 was not consistent with the Court's case-law in that it had not sought to ascertain whether the interference with his right to respect for his private life and correspondence had been in accordance with the law, had pursued a legitimate aim and had been necessary in a democratic society.

88. With regard to the jurisdiction of the labour courts, the applicant contended that they were competent to carry out a full review of the lawfulness and justification of the measure referred to them. It was for the courts to request the production of the necessary evidence and to raise any relevant factual or legal issues, even where they had not been mentioned by the parties. Accordingly, the labour courts had extensive jurisdiction to examine any issues relating to a labour-law dispute, including those linked to respect for employees' private life and correspondence.

89. However, in the applicant's case the domestic courts had pursued a rigid approach, aimed simply at upholding his employer's decision. They had performed an incorrect analysis of the factual aspects of the case and had failed to take into account the specific features of communications in cyberspace. The violation of the applicant's right to respect for his private life and correspondence had thus been intentional and illegal and its aim had been to gather evidence enabling his contract to be terminated.

90. Lastly, the applicant complained for the first time in the proceedings before the Grand Chamber of the outcome of the criminal complaint he had lodged in 2007: in 2012 the department of the prosecutor's office with

responsibility for investigating organised crime and terrorism (DIICOT) had rejected the complaint without properly establishing the facts of the case.

91. At the hearing before the Grand Chamber the applicant stated, in reply to a question from the judges, that because his employer had only made a single printer available to employees, all his colleagues had been able to see the contents of the forty-five-page transcript of his Yahoo Messenger communications.

92. The applicant urged the Grand Chamber to find a violation of Article 8 of the Convention and to take the opportunity to confirm that monitoring of employees' correspondence could only be carried out in compliance with the applicable legislation, in a transparent manner and on grounds provided for by law, and that employers did not have discretion to monitor their employees' correspondence.

(b) The Government

93. The Government stated that the employer had recorded the applicant's communications from 5 to 13 July 2007 and had then given him an opportunity to account for his internet use, which was more substantial than that of his colleagues. They pointed out that since the applicant had maintained that the contents of his communications were work-related, the employer had investigated his explanations.

94. The Government argued that in his appeal against the decision of the first-instance court the applicant had not challenged the court's finding that he had been informed that his employer was monitoring internet use. In that connection, they produced a copy of the information notice issued by the employer and signed by the applicant. On the basis of the employer's attendance register, they observed that the applicant had signed the notice between 3 and 13 July 2007.

95. The Government further submitted that the employer had recorded the applicant's communications in real time. There was no evidence that the employer had accessed the applicant's previous communications or his private email.

96. The Government indicated their agreement with the Chamber's conclusions and submitted that the Romanian State had satisfied its positive obligations under Article 8 of the Convention.

97. They observed firstly that the applicant had chosen to raise his complaints in the domestic courts in the context of a labour-law dispute. The courts had examined all his complaints and weighed up the various interests at stake, but the main focus of their analysis had been whether the disciplinary proceedings against the applicant had been compliant with domestic law. The applicant had had the option of raising before the domestic courts his specific complaint of a violation of his right to respect for his private life, for example by means of an action under Law no. 677/2001 or an action in tort, but he had chosen not to do so. He had

also filed a criminal complaint, which had given rise to a decision by the prosecuting authorities to take no further action on the grounds that the monitoring by the employer of employees' communications had not been unlawful.

98. Referring more specifically to the State's positive obligations, the Government submitted that approaches among Council of Europe member States varied greatly as regards the regulation of employee monitoring by employers. Some States included this matter within the wider scope of personal data processing, while others had passed specific legislation in this sphere. Even among the latter group of States, there were no uniform solutions regarding the scope and purpose of monitoring by the employer, prior notification of employees or personal internet use.

99. Relying on *Köpke* (cited above), the Government maintained that the domestic courts had performed an appropriate balancing exercise between the applicant's right to respect for his private life and correspondence and his employer's right to organise and supervise work within the company. In the Government's submission, where communications were monitored by a private entity, an appropriate examination by the domestic courts was sufficient for the purposes of Article 8 and there was no need for specific protection by means of a legislative framework.

100. The Government further submitted that the domestic courts had reviewed the lawfulness and the necessity of the employer's decision and had concluded that the disciplinary proceedings had been conducted in accordance with the legislation in force. They attached particular importance to the manner in which the proceedings had been conducted, especially the opportunity given to the applicant to indicate whether the communications in question had been private. If he had made use of that opportunity, the domestic courts would have weighed up the interests at stake differently.

101. In that connection, the Government noted that in the proceedings before the domestic authorities the applicant himself had produced the full transcripts of his communications, without taking any precautions; he could instead have disclosed only the names of the relevant accounts or submitted extracts of his communications, for example those that did not contain any intimate information. The Government also disputed the applicant's allegations that his communications had been disclosed to his colleagues and pointed out that only the three-member disciplinary board had had access to them.

102. The Government further contended that the employer's decision had been necessary, since it had had to investigate the arguments raised by the applicant in the disciplinary proceedings in order to determine whether he had complied with the internal regulations.

103. Lastly, the Government argued that a distinction should be made between the nature of the communications and their content. They observed,

as the Chamber had, that the domestic courts had not taken the content of the applicant's communications into account at all but had simply examined their nature and found that they were personal.

104. The Government thus concluded that the applicant's complaint under Article 8 of the Convention was ill-founded.

(c) Third parties

(i) The French Government

105. The French Government referred, in particular, to their conception of the scope of the national authorities' positive obligation to ensure respect for employees' private life and correspondence. They provided a comprehensive overview of the applicable provisions of French civil law, labour law and criminal law in this sphere. In their submission, Article 8 of the Convention was only applicable to strictly personal data, correspondence and electronic activities. In that connection, they referred to settled case-law of the French Court of Cassation to the effect that any data processed, sent and received by means of the employer's electronic equipment were presumed to be professional in nature unless the employee designated them clearly and precisely as personal.

106. The French Government submitted that States had to enjoy a wide margin of appreciation in this sphere since the aim was to strike a balance between competing private interests. The employer could monitor employees' professional data and correspondence to a reasonable degree, provided that a legitimate aim was pursued, and could use the results of the monitoring operation in disciplinary proceedings. They emphasised that employees had to be given advance notice of such monitoring. In addition, where data clearly designated as personal by the employee were involved, the employer could ask the courts to order investigative measures and to instruct a bailiff to access the relevant data and record their content.

(ii) The European Trade Union Confederation

107. The European Trade Union Confederation submitted that it was crucial to protect privacy in the working environment, taking into account in particular the fact that employees were structurally dependent on employers in this context. After summarising the applicable principles of international and European law, it stated that internet access should be regarded as a human right and that the right to respect for correspondence should be strengthened. The consent, or at least prior notification, of employees was required, and staff representatives had to be informed, before the employer could process employees' personal data.

2. The Court's assessment

(a) Whether the case concerns a negative or a positive obligation

108. The Court must determine whether the present case should be examined in terms of the State's negative or positive obligations. It reiterates that by Article 1 of the Convention, the Contracting Parties "shall secure to everyone within their jurisdiction the rights and freedoms defined in ... [the] Convention". While the essential object of Article 8 of the Convention is to protect individuals against arbitrary interference by public authorities, it may also impose on the State certain positive obligations to ensure effective respect for the rights protected by Article 8 (see, among other authorities, *X and Y v. the Netherlands*, 26 March 1985, § 23, Series A no. 91; *Von Hannover (no. 2)*, cited above, § 98; and *Hämäläinen v. Finland* [GC], no. 37359/09, § 62, ECHR 2014).

109. In the present case the Court observes that the measure complained of by the applicant, namely the monitoring of Yahoo Messenger communications, which resulted in disciplinary proceedings against him followed by his dismissal for infringing his employer's internal regulations prohibiting the personal use of company resources, was not taken by a State authority but by a private commercial company. The monitoring of the applicant's communications and the inspection of their content by his employer in order to justify his dismissal cannot therefore be regarded as "interference" with his right by a State authority.

110. Nevertheless, the Court notes that the measure taken by the employer was accepted by the national courts. It is true that the monitoring of the applicant's communications was not the result of direct intervention by the national authorities; however, their responsibility would be engaged if the facts complained of stemmed from a failure on their part to secure to the applicant the enjoyment of a right enshrined in Article 8 of the Convention (see, *mutatis mutandis*, *Obst v. Germany*, no. 425/03, §§ 40 and 43, 23 September 2010, and *Schüth v. Germany*, no. 1620/03, §§ 54 and 57, ECHR 2010).

111. In the light of the particular circumstances of the case as described in paragraph 109 above, the Court considers, having regard to its conclusion concerning the applicability of Article 8 of the Convention (see paragraph 81 above) and to the fact that the applicant's enjoyment of his right to respect for his private life and correspondence was impaired by the actions of a private employer, that the complaint should be examined from the standpoint of the State's positive obligations.

112. While the boundaries between the State's positive and negative obligations under the Convention do not lend themselves to precise definition, the applicable principles are nonetheless similar. In both contexts regard must be had in particular to the fair balance that has to be struck between the competing interests of the individual and of the community as a

whole, subject in any event to the margin of appreciation enjoyed by the State (see *Palomo Sánchez and Others v. Spain* [GC], nos. 28955/06 and 3 others, § 62, ECHR 2011).

(b) General principles applicable to the assessment of the State's positive obligation to ensure respect for private life and correspondence in an employment context

113. The Court reiterates that the choice of the means calculated to secure compliance with Article 8 of the Convention in the sphere of the relations of individuals between themselves is in principle a matter that falls within the Contracting States' margin of appreciation. There are different ways of ensuring respect for private life, and the nature of the State's obligation will depend on the particular aspect of private life that is at issue (see *Söderman v. Sweden* [GC], no. 5786/08, § 79, ECHR 2013, with further references).

114. The Court's task in the present case is therefore to clarify the nature and scope of the positive obligations that the respondent State was required to comply with in protecting the applicant's right to respect for his private life and correspondence in the context of his employment.

115. The Court observes that it has held that in certain circumstances, the State's positive obligations under Article 8 of the Convention are not adequately fulfilled unless it secures respect for private life in the relations between individuals by setting up a legislative framework taking into consideration the various interests to be protected in a particular context (see *X and Y v. the Netherlands*, cited above, §§ 23, 24 and 27, and *M.C. v. Bulgaria*, no. 39272/98, § 150, ECHR 2003-XII, both concerning sexual assaults of minors; see also *K.U. v. Finland*, no. 2872/02, §§ 43 and 49, ECHR 2008, concerning an advertisement of a sexual nature placed on an internet dating site in the name of a minor; *Söderman*, cited above, § 85, concerning the effectiveness of remedies in respect of an alleged violation of personal integrity committed by a close relative; and *Codarcea v. Romania*, no. 31675/04, §§ 102-04, 2 June 2009, concerning medical negligence).

116. The Court accepts that protective measures are not only to be found in labour law, but also in civil and criminal law. As far as labour law is concerned, it must ascertain whether in the present case the respondent State was required to set up a legislative framework to protect the applicant's right to respect for his private life and correspondence in the context of his professional relationship with a private employer.

117. In this connection it considers at the outset that labour law has specific features that must be taken into account. The employer-employee relationship is contractual, with particular rights and obligations on either side, and is characterised by legal subordination. It is governed by its own legal rules, which differ considerably from those generally applicable to

relations between individuals (see *Saumier v. France*, no. 74734/14, § 60, 12 January 2017).

118. From a regulatory perspective, labour law leaves room for negotiation between the parties to the contract of employment. Thus, it is generally for the parties themselves to regulate a significant part of the content of their relations (see, *mutatis mutandis*, *Wretlund v. Sweden* (dec.), no. 46210/99, 9 March 2004, concerning the compatibility with Article 8 of the Convention of the obligation for the applicant, an employee at a nuclear plant, to undergo drug tests; with regard to trade-union action from the standpoint of Article 11, see *Gustafsson v. Sweden*, 25 April 1996, § 45, *Reports* 1996-II, and, *mutatis mutandis*, *Demir and Baykara v. Turkey* [GC], no. 34503/97, §§ 140-46, ECHR 2008, for the specific case of civil servants). It also appears from the comparative-law material at the Court's disposal that there is no European consensus on this issue. Few member States have explicitly regulated the question of the exercise by employees of their right to respect for their private life and correspondence in the workplace (see paragraph 52 above).

119. In the light of the above considerations, the Court takes the view that the Contracting States must be granted a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace.

120. Nevertheless, the discretion enjoyed by States in this field cannot be unlimited. The domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse (see, *mutatis mutandis*, *Klass and Others v. Germany*, 6 September 1978, § 50, Series A no. 28, and *Roman Zakharov*, cited above, §§ 232-34).

121. The Court is aware of the rapid developments in this area. Nevertheless, it considers that proportionality and procedural guarantees against arbitrariness are essential. In this context, the domestic authorities should treat the following factors as relevant:

(*i*) whether the employee has been notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures. While in practice employees may be notified in various ways depending on the particular factual circumstances of each case, the Court considers that for the measures to be deemed compatible with the requirements of Article 8 of the Convention, the notification should normally be clear about the nature of the monitoring and be given in advance;

(*ii*) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy. In this regard, a distinction should be made between monitoring of the flow of communications and of their

content. Whether all communications or only part of them have been monitored should also be taken into account, as should the question whether the monitoring was limited in time and the number of people who had access to the results (see *Köpke*, cited above). The same applies to the spatial limits to the monitoring;

(*iii*) whether the employer has provided legitimate reasons to justify monitoring the communications and accessing their actual content (see paragraphs 38, 43 and 45 above for an overview of international and European law in this area). Since monitoring of the content of communications is by nature a distinctly more invasive method, it requires weightier justification;

(*iv*) whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications. In this connection, there should be an assessment in the light of the particular circumstances of each case of whether the aim pursued by the employer could have been achieved without directly accessing the full contents of the employee's communications;

(*v*) the consequences of the monitoring for the employee subjected to it (see, *mutatis mutandis*, the similar criterion applied in the assessment of the proportionality of an interference with the exercise of freedom of expression as protected by Article 10 of the Convention in *Axel Springer AG v. Germany* [GC], no. 39954/08, § 95, 7 February 2012, with further references); and the use made by the employer of the results of the monitoring operation, in particular whether the results were used to achieve the declared aim of the measure (see *Köpke*, cited above);

(*vi*) whether the employee had been provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature. Such safeguards should in particular ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality.

In this context, it is worth reiterating that in order to be fruitful, labour relations must be based on mutual trust (see *Palomo Sánchez and Others*, cited above, § 76).

122. Lastly, the domestic authorities should ensure that an employee whose communications have been monitored has access to a remedy before a judicial body with jurisdiction to determine, at least in substance, how the criteria outlined above were observed and whether the impugned measures were lawful (see *Obst*, cited above, § 45, and *Köpke*, cited above).

123. In the present case the Court will assess how the domestic courts to which the applicant applied dealt with his complaint of an infringement by his employer of his right to respect for his private life and correspondence in an employment context.

(c) Application of the above general principles in the present case

124. The Court observes that the domestic courts held that the interests at stake in the present case were, on the one hand, the applicant's right to respect for his private life, and on the other hand, the employer's right to engage in monitoring, including the corresponding disciplinary powers, in order to ensure the smooth running of the company (see paragraphs 28 and 30 above). It considers that, by virtue of the State's positive obligations under Article 8 of the Convention, the national authorities were required to carry out a balancing exercise between these competing interests.

125. The Court observes that the precise subject of the complaint brought before it is the alleged failure of the national courts, in the context of a labour-law dispute, to protect the applicant's right under Article 8 of the Convention to respect for his private life and correspondence in an employment context. Throughout the proceedings the applicant complained in particular, both before the domestic courts and before the Court, about his employer's monitoring of his communications via the Yahoo Messenger accounts in question and the use of their contents in the subsequent disciplinary proceedings against him.

126. As to whether the employer disclosed the contents of the communications to the applicant's colleagues (see paragraph 26 above), the Court observes that this argument is not sufficiently substantiated by the material in the case file and that the applicant did not produce any further evidence at the hearing before the Grand Chamber (see paragraph 91 above).

127. It therefore considers that the complaint before it concerns the applicant's dismissal based on the monitoring carried out by his employer. More specifically, it must ascertain in the present case whether the national authorities performed a balancing exercise, in accordance with the requirements of Article 8 of the Convention, between the applicant's right to respect for his private life and correspondence and the employer's interests. Its task is therefore to determine whether, in the light of all the circumstances of the case, the competent national authorities struck a fair balance between the competing interests at stake when accepting the monitoring measures to which the applicant was subjected (see, *mutatis mutandis*, *Palomo Sánchez and Others*, cited above, § 62). It acknowledges that the employer has a legitimate interest in ensuring the smooth running of the company, and that this can be done by establishing mechanisms for checking that its employees are performing their professional duties adequately and with the necessary diligence.

128. In the light of the above considerations, the Court will first examine the manner in which the domestic courts established the relevant facts in the present case. Both the County Court and the Court of Appeal held that the applicant had had prior notification from his employer (see paragraphs 28

and 30 above). The Court must then ascertain whether the domestic courts observed the requirements of the Convention when considering the case.

129. At this stage, the Court considers it useful to reiterate that when it comes to establishing the facts, it is sensitive to the subsidiary nature of its task and must be cautious in taking on the role of a first-instance tribunal of fact, where this is not rendered unavoidable by the circumstances of a particular case (see *Mustafa Tunç and Fecire Tunç v. Turkey* [GC], no. 24014/05, § 182, 14 April 2015). Where domestic proceedings have taken place, it is not the Court's task to substitute its own assessment of the facts for that of the domestic courts and it is for the latter to establish the facts on the basis of the evidence before them (see, among other authorities, *Edwards v. the United Kingdom*, 16 December 1992, § 34, Series A no. 247-B). Though the Court is not bound by the findings of domestic courts and remains free to make its own assessment in the light of all the material before it, in normal circumstances it requires cogent elements to lead it to depart from the findings of fact reached by the domestic courts (see *Giuliani and Gaggio v. Italy* [GC], no. 23458/02, § 180, ECHR 2011 (extracts), and *Aydan v. Turkey*, no. 16281/10, § 69, 12 March 2013).

130. The evidence produced before the Court indicates that the applicant had been informed of his employer's internal regulations, which prohibited the personal use of company resources (see paragraph 12 above). He had acknowledged the contents of the document in question and had signed a copy of it on 20 December 2006 (see paragraph 14 above). In addition, the employer had sent all employees an information notice dated 26 June 2007 reminding them that personal use of company resources was prohibited and explaining that an employee had been dismissed for breaching this rule (see paragraph 15 above). The applicant acquainted himself with the notice and signed a copy of it on an unspecified date between 3 and 13 July 2007 (see paragraph 16 above). The Court notes lastly that on 13 July 2007 the applicant was twice summoned by his employer to provide explanations as to his personal use of the internet (see paragraphs 18 and 20 above). Initially, after being shown the charts indicating his internet activity and that of his colleagues, he argued that his use of his Yahoo Messenger account had been purely work-related (see paragraphs 18 and 19 above). Subsequently, on being presented fifty minutes later with a forty-five-page transcript of his communications with his brother and fiancée, he informed his employer that in his view it had committed the criminal offence of breaching the secrecy of correspondence (see paragraph 22 above).

131. The Court notes that the domestic courts correctly identified the interests at stake – by referring explicitly to the applicant's right to respect for his private life – and also the applicable legal principles (see paragraphs 28 and 30 above). In particular, the Court of Appeal made express reference to the principles of necessity, purpose specification, transparency, legitimacy, proportionality and security set forth in Directive 95/46/EC, and

pointed out that the monitoring of internet use and of electronic communications in the workplace was governed by those principles (see paragraph 30 above). The domestic courts also examined whether the disciplinary proceedings had been conducted in an adversarial manner and whether the applicant had been given the opportunity to put forward his arguments.

132. It remains to be determined how the national authorities took the criteria set out above (see paragraph 121) into account in their reasoning when weighing the applicant's right to respect for his private life and correspondence against the employer's right to engage in monitoring, including the corresponding disciplinary powers, in order to ensure the smooth running of the company.

133. As to whether the applicant had received prior notification from his employer, the Court observes that it has already concluded that he did not appear to have been informed in advance of the extent and nature of his employer's monitoring activities, or of the possibility that the employer might have access to the actual content of his messages (see paragraph 78 above). With regard to the possibility of monitoring, it notes that the County Court simply observed that "the employees' attention had been drawn to the fact that, shortly before the applicant's disciplinary sanction, another employee had been dismissed" (see paragraph 28 above) and that the Court of Appeal found that the applicant had been warned that he should not use company resources for personal purposes (see paragraph 30 above). Accordingly, the domestic courts omitted to determine whether the applicant had been notified in advance of the possibility that the employer might introduce monitoring measures, and of the scope and nature of such measures. The Court considers that to qualify as prior notice, the warning from the employer must be given before the monitoring activities are initiated, especially where they also entail accessing the contents of employees' communications. International and European standards point in this direction, requiring the data subject to be informed before any monitoring activities are carried out (see paragraphs 38 and 43 above; see also, for a comparative-law perspective, paragraph 53 above).

134. As regards the scope of the monitoring and the degree of intrusion into the applicant's privacy, the Court observes that this question was not examined by either the County Court or the Court of Appeal (see paragraphs 28 and 30 above), even though it appears that the employer recorded all the applicant's communications during the monitoring period in real time, accessed them and printed out their contents (see paragraphs 17 and 21 above).

135. Nor does it appear that the domestic courts carried out a sufficient assessment of whether there were legitimate reasons to justify monitoring the applicant's communications. The Court is compelled to observe that the Court of Appeal did not identify what specific aim in the present case could

have justified such strict monitoring. Admittedly, this question had been touched upon by the County Court, which had mentioned the need to avoid the company's IT systems being damaged, liability being incurred by the company in the event of illegal activities in cyberspace, and the company's trade secrets being disclosed (see paragraph 28 above). However, in the Court's view, these examples can only be seen as theoretical, since there was no suggestion that the applicant had actually exposed the company to any of those risks. Furthermore, the Court of Appeal did not address this question at all.

136. In addition, neither the County Court nor the Court of Appeal sufficiently examined whether the aim pursued by the employer could have been achieved by less intrusive methods than accessing the actual contents of the applicant's communications.

137. Moreover, neither court considered the seriousness of the consequences of the monitoring and the subsequent disciplinary proceedings. In this respect the Court notes that the applicant had received the most severe disciplinary sanction, namely dismissal.

138. Lastly, the Court observes that the domestic courts did not determine whether, when the employer summoned the applicant to give an explanation for his use of company resources, in particular the internet (see paragraphs 18 and 20 above), it had in fact already accessed the contents of the communications in issue. It notes that the national authorities did not establish at what point during the disciplinary proceedings the employer had accessed the relevant content. In the Court's view, accepting that the content of communications may be accessed at any stage of the disciplinary proceedings runs counter to the principle of transparency (see, to this effect, Recommendation CM/Rec(2015)5, cited in paragraph 43 above; for a comparative-law perspective, see paragraph 54 above).

139. Having regard to the foregoing, the Court finds that the Court of Appeal's conclusion that a fair balance was struck between the interests at stake (see paragraph 30 above) is questionable. Such an assertion appears somewhat formal and theoretical. The Court of Appeal did not explain the specific reasons linked to the particular circumstances of the applicant and his employer that led it to reach that finding.

140. That being so, it appears that the domestic courts failed to determine, in particular, whether the applicant had received prior notice from his employer of the possibility that his communications on Yahoo Messenger might be monitored; nor did they have regard either to the fact that he had not been informed of the nature or the extent of the monitoring, or to the degree of intrusion into his private life and correspondence. In addition, they failed to determine, firstly, the specific reasons justifying the introduction of the monitoring measures; secondly, whether the employer could have used measures entailing less intrusion into the applicant's private life and correspondence; and thirdly, whether the communications

might have been accessed without his knowledge (see paragraphs 120 and 121 above).

141. Having regard to all the above considerations, and notwithstanding the respondent State's margin of appreciation, the Court considers that the domestic authorities did not afford adequate protection of the applicant's right to respect for his private life and correspondence and that they consequently failed to strike a fair balance between the interests at stake. There has therefore been a violation of Article 8 of the Convention.

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

142. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

1. Pecuniary damage

143. Before the Chamber, the applicant claimed 59,976.12 euros (EUR) in respect of the pecuniary damage he had allegedly sustained. He explained that this amount represented the current value of the wages to which he would have been entitled if he had not been dismissed. At the hearing before the Grand Chamber, the applicant's representatives stated that they maintained their claim for just satisfaction.

144. In their observations before the Chamber, the Government stated that they were opposed to any award in respect of the pecuniary damage alleged to have been sustained. In their submission, the sum claimed was based on mere speculation and there was no link between the applicant's dismissal and the damage alleged.

145. The Court observes that it has found a violation of Article 8 of the Convention in that the national courts failed to establish the relevant facts and to perform an adequate balancing exercise between the applicant's right to respect for his private life and correspondence and the employer's interests. It does not discern any causal link between the violation found and the pecuniary damage alleged, and therefore dismisses this claim.

2. Non-pecuniary damage

146. Before the Chamber, the applicant also claimed EUR 200,000 in respect of the non-pecuniary damage he had allegedly sustained as a result of his dismissal. He stated that because of the disciplinary nature of the dismissal, he had been unable to find another job, that his standard of living

had consequently deteriorated, that he had lost his social standing and that as a result, his fiancée had decided in 2010 to end their relationship.

147. The Government submitted in reply that the finding of a violation could in itself constitute sufficient just satisfaction. In any event, they submitted that the sum claimed by the applicant was excessive in the light of the Court's case-law in this area.

148. The Court considers that the finding of a violation constitutes sufficient just satisfaction for any non-pecuniary damage that may have been sustained by the applicant.

B. Costs and expenses

149. Before the Chamber, the applicant also claimed 3,310 Romanian lei (RON) (approximately EUR 750) in respect of the costs and expenses incurred in the domestic courts, and RON 500 (approximately EUR 115) for the fees of the lawyer who had represented him in the domestic proceedings. He claimed a further EUR 500 for the fees of the lawyers who had represented him before the Court. He produced the following in support of his claim:

- copies of the legal-aid agreement and of the receipt for payment of the sum of RON 500, corresponding to his lawyer's fees in the domestic proceedings;
- documents proving that he had paid his employer the sums of RON 2,700 and RON 610.30 in respect of costs and expenses;
- a copy of the receipt for payment of the sum of RON 2,218.64, corresponding to the fees of one of the lawyers who had represented him before the Court.

The applicant did not seek the reimbursement of the expenses incurred in connection with the proceedings before the Grand Chamber.

150. In their observations before the Chamber, the Government requested the Court to award the applicant only those sums that were necessary and corresponded to duly substantiated claims. In that connection, they submitted that the applicant had not proved that he had paid EUR 500 in fees to the lawyers who had represented him before the Court, and that the receipt for payment of a sum of RON 500 in fees to the lawyer who had represented him in the domestic courts had not been accompanied by any supporting documents detailing the hours worked.

151. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum (see *Lupeni Greek Catholic Parish and Others v. Romania* [GC], no. 76943/11, § 187, ECHR 2016 (extracts)). In the present case, having regard to the documents in its possession and to its case-law, the Court considers it reasonable to award the applicant the sum of EUR 1,365

covering costs under all heads.

C. Default interest

152. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT

1. *Holds*, by eleven votes to six, that there has been a violation of Article 8 of the Convention;

2. *Holds*, by sixteen votes to one, that the finding of a violation constitutes in itself sufficient just satisfaction for the non-pecuniary damage sustained by the applicant;

3. *Holds*, by fourteen votes to three,
   (a) that the respondent State is to pay the applicant, within three months, EUR 1,365 (one thousand three hundred and sixty-five euros) in respect of costs and expenses, to be converted into the currency of the respondent State at the rate applicable at the date of settlement, plus any tax that may be chargeable to the applicant;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

4. *Dismisses*, unanimously, the remainder of the applicant's claim for just satisfaction.

Done in English and French, and delivered at a public hearing in the Human Rights Building, Strasbourg, on 5 September 2017.

Søren Prebensen
Deputy to the Registrar

Guido Raimondi
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) partly dissenting opinion of Judge Karakaş;

(b) joint dissenting opinion of Judges Raimondi, Dedov, Kjølbro, Mits, Mourou-Vikström and Eicke.

G.R.
S.C.P.

PARTLY DISSENTING OPINION OF JUDGE KARAKAŞ

(Translation)

I agree entirely with the majority's finding of a violation of Article 8 of the Convention.

However, I do not share the majority's opinion that the finding of a violation constitutes sufficient just satisfaction for the non-pecuniary damage sustained by the applicant.

It is obvious that under Article 41 the Court decides to award a certain amount in respect of non-pecuniary damage if it considers it "necessary" to afford redress. As it has considerable latitude to determine in which cases such an award should be made to the applicants, the Court sometimes concludes that the finding of a violation constitutes sufficient just satisfaction and that no monetary award is required (see, among many other authorities, *Nikolova v. Bulgaria*, no. 31195/96, § 76, ECHR 1999-II; *Vinter and Others v. the United Kingdom* [GC], nos. 66069/09 and 2 others, ECHR 2013 (extracts); and *Murray v. the Netherlands* [GC], no. 10511/10, ECHR 2016). In order to arrive at that conclusion, the Court will have regard to all the facts of the case, including the nature of the violations found and any special circumstances pertaining to the context of the case (see, for example, *Vinter and Others*, cited above, and the joint partly dissenting opinion of Judges Spielmann, Sajó, Karakaş and Pinto de Albuquerque in the case of *Murray*, cited above). Where this is warranted by the circumstances of the case, as in *McCann and Others v. the United Kingdom* (27 September 1995, § 219, Series A no. 324), in which the Court declined to make any award in respect of non-pecuniary damage in view of the fact that the three terrorist suspects who had been killed had been intending to plant a bomb in Gibraltar, or by the nature of the violation found, as in the case of *Tarakhel v. Switzerland* ([GC], no. 29217/12, ECHR 2014 (extracts)), the Court rules that the finding of a violation in itself affords sufficient just satisfaction for any non-pecuniary damage. In other words, it is only in very exceptional cases that the Court decides not to make any award in respect of non-pecuniary damage.

There may also be instances in which the Court decides to award a lower sum than that awarded in other cases relating to the Article concerned, again taking into consideration the particular features of the context. For example, in *A. and Others v. the United Kingdom* ([GC], no. 3455/05, ECHR 2009), in the context of terrorism, the Court gave detailed reasons (§ 252; see also *Del Río Prada v. Spain* [GC], no. 42750/09, § 145, ECHR 2013) explaining why it had awarded a significantly lower sum than in other previous cases concerning unlawful detention.

In the present case, the domestic courts did not ensure adequate protection of the applicant's right to respect for his private life and

correspondence: the applicant was seriously affected by the disciplinary proceedings against him, since he was dismissed from his post.

This violation of Article 8 undoubtedly caused non-pecuniary damage to the applicant, who cannot be satisfied with the mere finding that such damage was sustained. For that reason, I was in favour of granting an award, even of a modest amount, by way of just satisfaction for the non-pecuniary damage sustained by the applicant.

JOINT DISSENTING OPINION OF JUDGES RAIMONDI, DEDOV, KJØLBRO, MITS, MOUROU-VIKSTRÖM AND EICKE

Introduction

1. We agree with the majority, some of us with some hesitation, that, even in a context where on the facts before the Court it is difficult to see how the applicant could have had a "reasonable expectation of privacy" (see below), Article 8 is applicable in the circumstances of this case (see paragraphs 69 to 81 of the judgment). With Article 8 having been found to be applicable, we also agree that this applicant's complaint falls to be examined from the standpoint of the State's positive obligations (see paragraph 111 of the judgment). Subject to what follows, we also agree with the general principles applicable to the assessment of the State's positive obligation, as set out in paragraphs 113 to 122 of the judgment.

2. However, for the reasons set out below, we respectfully disagree with the majority in relation to the correct approach to the State's positive obligation in the context of this case and their ultimate conclusion that the "domestic authorities", by which the majority means only the employment courts, "did not afford adequate protection of the applicant's right to respect for his private life and correspondence and that they consequently failed to strike a fair balance between the interests at stake" (see paragraph 141 of the judgment).

Principle

3. In light of the fact that there is common ground that the present application is to be considered by reference to the State's positive obligation under Article 8, the appropriate starting point is provided by the Court's case-law defining the content and reach of the concept of "positive obligations" under Article 8. The relevant principles were most recently summarised by the Grand Chamber, in the context of the positive obligation to protect the applicant's physical and psychological integrity from other persons, in *Söderman v. Sweden* ([GC], no. 5786/08, §§ 78-85, ECHR 2013). There the Court made clear that:

> (a) the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities. However, this provision does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there are positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of

the relations of individuals between themselves (see, *inter alia*, *Airey v. Ireland*, 9 October 1979, § 32, Series A no. 32) (*Söderman*, cited above, § 78);

(b) the choice of the means calculated to secure compliance with Article 8 of the Convention in the sphere of the relations of individuals between themselves is in principle a matter that falls within the Contracting States' margin of appreciation, whether the obligations on the State are positive or negative. There are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is in issue (see, for example, *Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, § 104, ECHR 2012; *Odièvre v. France* [GC], no. 42326/98, § 46, ECHR 2003‑III; *Evans v. the United Kingdom* [GC], no. 6339/05, § 77, ECHR 2007‑I; and *Mosley v. the United Kingdom*, no. 48009/08, § 109, 10 May 2011) (*Söderman*, cited above, § 79); and

(c) in respect of less serious acts between individuals, which may violate psychological integrity, the obligation of the State under Article 8 to maintain and apply in practice an adequate legal framework affording protection does not always require that an efficient criminal-law provision covering the specific act be in place. The legal framework could also consist of civil-law remedies capable of affording sufficient protection (see, *mutatis mutandis*, *X and Y v. the Netherlands*, 26 March 1985, §§ 24 and 27, Series A no. 91, and *K.U. v. Finland*, no. 2872/02, § 47, ECHR 2008). The Court notes, for example, that in some previous cases concerning the protection of a person's picture against abuse by others, the remedies available in the member States have been of a civil-law nature, possibly combined with procedural remedies such as the granting of an injunction (see, *inter alia*, *Von Hannover*, cited above; *Reklos and Davourlis v. Greece*, no. 1234/05, 15 January 2009; and *Schüssel v. Austria* (dec.), no. 42409/98, 21 February 2002) (*Söderman*, cited above, § 85).

4. The facts of this case, as the majority at least implicitly accepts (see paragraph 80 of the judgment), are, of course, a million miles away from the seriousness of the cases considered in *Söderman*. After all, in that case the Court was concerned with allegations of the violation of a person's physical or psychological integrity by another person.

5. Nevertheless, even in that context, it is clear, firstly, that the choice of measures designed to secure respect for private life under Article 8, even in the sphere of the relations of individuals between themselves, is primarily for the Contracting States; a choice in relation to which they enjoy a wide margin of appreciation (see paragraph 119 of the judgment; narrowing where, unlike in the present case, a particularly important facet of an individual's existence or identity is at stake, or where the activities at stake involve a most intimate aspect of private life). This conclusion is underlined

by the fact that there is no European consensus on this matter and only six out of thirty-four surveyed Council of Europe member States have explicitly regulated the issue of the workplace privacy (see paragraphs 52 and 118 of the judgment). Secondly, the "measures" adopted by the State under Article 8 should in principle take the form of an adequate "legal framework" affording protection to the victim. Article 8 does not necessarily require that an efficient criminal-law provision covering the specific act be in place. The legal framework could also consist of civil-law remedies capable of affording sufficient protection.

6. This, of course, applies *mutatis mutandis* in the present case where, as the majority identify, the Court is at best concerned with the protection of a core or minimum level of private life and correspondence in the work place against interference by a private law employer.

The focus of the enquiry

7. Having identified some of the principles set out above, the majority, in paragraph 123, unjustifiably in our view, narrowed its enquiry to the question "how the domestic courts to which the applicant applied dealt with his complaint of an infringement by his employer of his right to respect for private life and correspondence in an employment context".

8. Although recognising that "protective measures are not only to be found in labour law, but also in civil and criminal law" (see paragraph 116 of the judgment), the majority in fact sidelined and avoided the real question that falls to be answered, namely: did the High Contracting Party maintain and apply an adequate "legal framework" providing at least civil-law remedies capable of affording sufficient protection to the applicant?

9. As the respondent Government submitted, and the majority accepts, the relevant "legal framework" in Romania consisted not only of the employment courts, before which the applicant raised his complaint, but also included *inter alia*:

(a) the criminal offence of "breach of secrecy of correspondence" under Article 195 of the Criminal Code (see paragraph 33 of the judgment); incidentally, a remedy which the applicant engaged by lodging a criminal complaint but, following a decision by the prosecutor that there was no case to answer, failed to exhaust by not challenging that decision in the domestic courts: paragraph 31 of the judgment;

(b) the provisions of Law no. 677/2001 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" (see paragraph 36 of the judgment), which, in anticipation of Romania's accession to the EU, reproduces certain provisions of Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free

movement of such data. This Law expressly provides, in Article 18, for a right to (i) lodge a complaint with the supervisory authority and, in the alternative or subsequently, (ii) apply to the competent courts for protection of the data protection rights safeguarded by the Act, including a right to seek compensation in relation to any damage suffered; and

(c) the provisions of the Civil Code (Articles 998 and 999; paragraph 34 of the judgment) enabling a claim in tort to be brought with a view to obtaining reparation for the damage caused, whether deliberately or through negligence.

10. Other than the criminal complaint which was not pursued any further, none of the domestic remedies was ever engaged by the applicant. Instead, the applicant only applied to the employment courts to challenge not primarily the interference by his employer with his private life/correspondence but his dismissal. As the majority note in paragraph 24:

> "He asked the court, firstly, to set aside the dismissal; secondly, to order his employer to pay him the amounts he was owed in respect of wages and any other entitlements and to reinstate him in his post; and thirdly, to order the employer to pay him 100,000 Romanian lei (approximately 30,000 euros) in damages for the harm resulting from the manner of his dismissal, and to reimburse his costs and expenses."

11. It was only in the context of these dismissal proceedings that, relying on the judgment of this Court in *Copland v. the United Kingdom* (no. 62617/00, §§ 43-44, ECHR 2007-I), he argued that the decision to dismiss him was unlawful and that by monitoring his communications and accessing their contents his employer had infringed criminal law.

12. The fact that the applicant's focus was primarily, if not exclusively, on the legality of his dismissal, rather than the interference by his employer with his right to respect for private life/correspondence, is also reflected in the way his case was presented before this Court. As the judgment notes at paragraph 55, the applicant's complaint was that "his dismissal by his employer had been based on a breach of his right to respect for his private life and correspondence and that, by not revoking that measure, the domestic courts had failed to comply with their obligation to protect the right in question".

13. As a consequence, one cannot help but note (if only in passing) that, if the respondent Government had raised this as a preliminary objection, there might have been some question as to whether, by applying to the employment courts on the basis he did, the applicant had, in fact, exhausted those domestic remedies "that relate to the breaches alleged and which are at the same time available and sufficient" (see *Aquilina v. Malta* [GC], no. 25642/94, § 39, ECHR 1999-III). After all, there is no material before the Court to suggest that any of the three remedies identified above, and, in particular, a complaint to the specialist data protection supervisory authority and/or an action for damages under Law no. 677/2001 before the competent

courts were "bound to fail" (see *Davydov and Others v. Russia*, no. 75947/11, § 233, 30 May 2017).

14. Our doubts about the effectiveness of the employment courts in this context (and the appropriateness of the Court restricting its analysis to the adequacy of the analysis by those employment courts) is further underlined by the fact that, in line with this Court's jurisprudence under Article 6 of the Convention, regardless of whether or not the employer's actions were illegal that fact could not *per se* undermine the validity of the disciplinary proceedings in the instant case. After all, as this Court confirmed most recently in *Vukota-Bojić v. Switzerland* (no. 61838/10, §§ 94-95, 18 October 2016):

> "... the question whether the use as evidence of information obtained in violation of Article 8 rendered a trial as a whole unfair contrary to Article 6 has to be determined with regard to all the circumstances of the case, including respect for the applicant's defence rights and the quality and importance of the evidence in question (compare, *inter alia*, *Khan*, cited above, §§ 35-40; *P.G. and J.H. v. the United Kingdom*, cited above, §§ 77-79; and *Bykov v. Russia* [GC], no. 4378/02, §§ 94-98, 10 March 2009, in which no violation of Article 6 was found).
>
> In particular, it must be examined whether the applicant was given an opportunity to challenge the authenticity of the evidence and to oppose its use. In addition, the quality of the evidence must be taken into consideration, as must the circumstances in which it was obtained and whether these circumstances cast doubts on its reliability or accuracy. Finally, the Court will attach weight to whether the evidence in question was or was not decisive for the outcome of the proceedings (compare, in particular, *Khan*, cited above, §§ 35 and 37)."

15. In any event, the above alternative domestic remedies, some of which are more obviously suitable to the protection of an individual's private life/correspondence in the private workplace, were plainly relevant to the assessment whether the "legal framework" created by Romania was capable of providing "adequate" protection to the applicant against an unlawful interference with his right to respect for private life/correspondence under Article 8 by another private individual (in this case, his employer).

16. By not including them, sufficiently or at all, in their analysis, the majority failed to have regard to important factors relevant to the question posed by this case and failed to give due weight to the acknowledged wide margin of appreciation enjoyed by High Contracting Parties in determining what measures to take and what remedies to provide for in compliance with their positive obligation under Article 8 to put in place an adequate "legal framework". Absent any evidence to suggest that the domestic remedies either individually or cumulatively were not sufficiently available or effective to provide the protection required under Article 8, it seems to us that there is no basis on which the Court could find a violation of Article 8 in the circumstances of the present case.

17. Before leaving this question of the appropriate focus for the enquiry, we would want to express our sincere hope that the majority judgment should not be read as a blanket requirement under the Convention that, where more appropriate remedies are available within the domestic legal framework (such as e.g. those required to be put in place under the relevant EU data protection legislation), the domestic employment courts, when confronted with a case such as that brought by the applicant, are required to duplicate the functions of any such, more appropriate, specialist remedy.

The analysis by the domestic employment courts

18. However, even if, contrary to the above, the majority's focus only on the analysis by the domestic employment courts were the appropriate approach, we also do not agree that, in fact, that analysis is defective so as to lead to a finding of a violation under Article 8.

19. In considering the judgments of the County Court and the Bucharest Court of Appeal, we note that both domestic courts took into consideration the employer's internal regulations, which prohibited the use of company resources for personal purposes (see paragraphs 12, 28 and 30 of the judgment). We further observe that the applicant had been informed of the internal regulations, since he had acquainted himself with them and signed a copy of them on 20 December 2006 (see paragraph 14 of the judgment). The domestic courts interpreted the provisions of that instrument as implying that it was possible that measures might be taken to monitor communications, an eventuality that was likely to reduce significantly the likelihood of any reasonable expectation on the applicant's part that the privacy of his correspondence would be respected (contrast *Halford v. the United Kingdom*, 25 June 1997, § 45, *Reports of Judgments and Decisions* 1997-III, and *Copland*, cited above, § 42). We therefore consider that the question of prior notification should have been examined against this background.

20. In this context, it is clear on the evidence before the Court that the domestic courts did indeed consider this question. Both the County Court and the Court of Appeal attached a certain weight to the information notice which the applicant had signed, and their decisions indicate that a signed copy of the notice was produced in the proceedings before them (see paragraphs 28 and 30 of the judgment). The County Court observed, among other things, that the employer had warned its employees that their activities, including their computer use, were being monitored, and that the applicant himself had acknowledged the information notice (see paragraph 28 of the judgment). The Court of Appeal further confirmed that "personal use [of company resources could] be refused ... in accordance with the provisions of the internal regulations", of which the employees had been duly informed (see paragraph 30 of the judgment). Accordingly, the

domestic courts found, on the basis of the documents in their possession, that the applicant had received sufficient warning that his activities, including his use of the computer made available to him by his employer, could be monitored. We can see no basis for departing from their decisions, and consider that the applicant could reasonably have expected his activities to be monitored.

21. Next, we note that the national authorities carried out a careful balancing exercise between the interests at stake, taking into account both the applicant's right to respect for his private life and the employer's right to engage in monitoring, including the corresponding disciplinary powers, in order to ensure the smooth running of the company (see paragraphs 28 and 30 of the judgment; see also, *mutatis mutandis*, *Obst v. Germany*, no. 425/03, § 49, 23 September 2010, and *Fernández Martínez v. Spain* [GC], no. 56030/07, § 151, ECHR 2014 (extracts). The Court of Appeal, in particular, citing the provisions of Directive 95/46/EC, noted that there had been a conflict in the present case between "the employer's right to engage in monitoring and the employees' right to protection of their privacy" (see paragraph 30 of the judgment).

22. We also note that, on the basis of the material in their possession, the domestic courts found that the legitimate aim pursued by the employer in engaging in the monitoring of the applicant's communications had been to exercise "the right and the duty to ensure the smooth running of the company" (see the Court of Appeal as quoted at paragraph 30 of the judgment). While the domestic courts attached greater weight to the employer's right to ensure the smooth running of the company and to supervise how employees performed their tasks in the context of their employment relationship than to the applicant's right to respect for his private life and correspondence, we consider that it is not unreasonable for an employer to wish to check that its employees are carrying out their professional duties when making use in the workplace and during working hours of the equipment which it has made available to them. The Court of Appeal found that the monitoring of the applicant's communications was the only way for the employer to achieve this legitimate aim, prompting it to conclude that a fair balance had been struck between the need to protect the applicant's private life and the employer's right to supervise the operation of its business (see paragraph 30 of the judgment).

23. In our view, the choice of the national authorities to give the employer's interests precedence over those of the employee is not capable in itself of raising an issue under the Convention (see, *mutatis mutandis*, *Obst*, cited above, § 49). We would reiterate that where they are required to strike a balance between several competing private interests, the authorities enjoy a certain discretion (see *Hämäläinen v. Finland* [GC], no. 37359/09, § 67 in fine, ECHR 2014, and further references). In the present case,

therefore, it is our view that the domestic courts acted within Romania's margin of appreciation.

24. We further note that the monitoring to which the applicant was subjected was limited in time, and that the evidence before the Court indicates that the employer only monitored the applicant's electronic communications and internet activity. Indeed, the applicant did not allege that any other aspect of his private life, as enjoyed in a professional context, had been monitored by his employer. Furthermore, on the evidence before the Court, the results of the monitoring operation were used solely for the purposes of the disciplinary proceedings against the applicant and only the persons involved in those proceedings had access to the content of the applicant's communications (for a similar approach see *Köpke v. Germany* (dec.), no. 420/07, 5 October 2010). In this connection, it is observed that the majority agree that the applicant did not substantiate his allegations that the content in question had been disclosed to other colleagues (see paragraph 126 of the judgment).

25. Lastly, we note that in their examination of the case, the national authorities took into account the attitude displayed by the applicant in the course of his professional activities in general, and during the disciplinary proceedings against him in particular. Thus, the County Court found that he had committed a disciplinary offence by breaching his employer's internal regulations, which prohibited the use of computers for personal purposes (see paragraph 28 of the judgment). The domestic authorities attached significant weight in their analysis to the applicant's attitude in the disciplinary proceedings, during which he had denied using his employer's resources for personal purposes and had maintained that he had used them solely for work-related purposes, which was incorrect (see paragraphs 28 and 30 of the judgment). They were plainly entitled to do so. This was confirmed when the applicant asserted before this Court that, despite the fact that he knew that private use of his work computer was prohibited, it would only have been an awareness of monitoring by the employer which would have led him not to engage in private use of the employer's computer; he did not deny that he was informed about the monitoring, but could not remember when he had received the information notice alerting him to the monitoring.

26. After all, as the majority also stress (see paragraph 121 of the judgment), in order to be fruitful, employment relations must be based on mutual trust (see *Palomo Sánchez and Others v. Spain* [GC], nos. 28955/06 and 3 others, § 76, ECHR 2011). Accordingly, it is our view that within their margin of appreciation, the domestic (employment) courts were entitled, when weighing up the interests at stake, to take into account the attitude displayed by the applicant, who had broken the bond of trust with his employer.

27. Having regard to all the foregoing considerations and in contrast to the majority, we conclude that there has been no failure to protect the applicant's right to respect for his private life and correspondence and that there has, therefore, been no violation of Article 8 of the Convention.

Recommendation CM/Rec(2015)5

of the Committee of Ministers to member States

on the processing of personal data in the context of employment

(Adopted by the Committee of Ministers on 1 April 2015,

at the 1224th meeting of the Ministers' Deputies)

The Committee of Ministers, under the terms of Article 15.*b* of the Statute of the Council of Europe,

Considering that the aim of the Council of Europe is to achieve a greater unity among its members;

Aware of the increasing use of new technologies and means of electronic communication in the relations between employers and employees, and the corresponding advantages thereof;

Believing, however, that the use of data-processing methods by employers should be guided by principles designed to minimise any risks that such methods might pose to employees' rights and fundamental freedoms, in particular their right to privacy;

Bearing in mind the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981 (ETS No. 108, hereinafter the "Convention No. 108") and of its Additional Protocol regarding supervisory authorities and transborder data flows of 8 November 2001 (ETS No. 181), and the desirability of applying the principles to the employment sector;

Recognising also that the interests to be borne in mind when developing principles for the employment sector are individual or collective, private or public;

Considering that personal data in official documents held by a public authority or a public body may be disclosed by the authority or body in accordance with the domestic law to which the public authority or body is subject, thus reconciling access to such official documents with the right to the protection of personal data in accordance with the principles of the present recommendation;

Aware of the different traditions which exist in member States with respect to the regulation of different aspects of employer-employee relations, and noting that law is only one of the means to regulate such relations;

Aware of the changes which have occurred internationally in the employment sector and related activities, notably due to the increased use of information and communication technologies (ICTs) and the globalisation of employment and services;

Considering that, in light of such changes, Recommendation Rec(89)2 of the Committee of Ministers to member States on the protection of personal data used for

employment purposes should be revised in order to continue to provide an adequate level of protection for individuals in the context of employment;

Recalling that Article 8 of the European Convention on Human Rights (ETS No. 5) protects the right to private life, including activities of a professional or business nature, as interpreted by the European Court of Human Rights;

Recalling the applicability of the existing principles set out in other relevant recommendations of the Committee of Ministers of the Council of Europe to member States, in particular Recommendation CM/Rec(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation Rec(97)5 on the protection of medical data and Recommendation Rec(92)3 on genetic testing and screening for health care purposes;

Recalling the Guiding Principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance, adopted by the European Committee on Legal Co-operation (CDCJ) of the Council of Europe in May 2003, referred to in Resolution 1604 (2008) on video surveillance of public areas of the Parliamentary Assembly of the Council of Europe, which are especially relevant;

Recalling the European Social Charter (ETS No. 163), as revised on 3 May 1996, and the International Labour Office's 1997 Code of practice on the protection of workers' personal data,

Recommends that governments of member States:

– ensure that the principles contained in the appendix to the present recommendation, which replaces the above-mentioned Recommendation Rec(89)2, are reflected in the application of domestic legislation on data protection in the employment sector, as well as in other branches of law which have a bearing on the use of personal data for employment purposes;

– for this purpose, ensure that the present recommendation and its appendix are brought to the attention of the authorities established under domestic data protection legislation which are competent to supervise the implementation of such legislation;

– promote the acceptance and implementation of the principles contained in the appendix to the present recommendation by means of complementary instruments, such as codes of conduct, to ensure that the principles are well known, understood and applied by all employment sector participants, including representative bodies of both employers and employees, and are taken into account in the design and use of ICTs in the employment sector.

Appendix to the Recommendation CM/Rec(2015)5

Part I – General principles

1. Scope

1.1. The principles set out in the present recommendation apply to any processing of personal data for employment purposes in both the public and private sectors.

1.2. Unless domestic law provides otherwise, the principles of the present recommendation also apply to the activities of employment agencies, whether in the public or private sector, which process personal data so as to enable one or more concurrent contracts of employment, including part-time contracts, to be established between individuals concerned and prospective employers, or to help employers discharge their duties relating to those contracts.

2. Definitions

For the purposes of the present recommendation:

"Personal data" means any information relating to an identified or identifiable individual ("data subject");

"Data processing" means any operation or set of operations which is performed upon personal data, and in particular the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure or destruction of data, or the carrying out of logical and/or arithmetical operations on data; where no automated processing is used, data processing means the operations carried out within a structured set established according to any criteria which allows for the search of personal data;

"Information systems" means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purpose of their operation, use, protection or maintenance;

"Employment purposes" concerns the relations between employers and employees which relate to recruitment, fulfilment of the contract of employment, management, including discharge of obligations laid down by law or laid down in collective agreements, as well as the planning and efficient running of an organisation and termination of the employment relationship. The consequences of the contractual relationship may extend beyond the term of the contract of employment;

"Employer" means any natural or legal person, public authority or agency that has an employment relationship with an employee or is considering such a relationship in respect of a job applicant and has the legal responsibility for the undertaking or establishment;

"Employee" means any natural person concerned under an employment relationship engaged by an employer.

3. Respect for human rights, dignity and fundamental freedoms

Respect for human dignity, privacy and the protection of personal data should be safeguarded in the processing of personal data for employment purposes, notably to allow for the free development of the employee's personality as well as for possibilities of individual and social relationships in the workplace.

4. Application of data processing principles

4.1. Employers should minimise the processing of personal data to only the data necessary to the aim pursued in the individual cases concerned.

4.2. Employers should develop appropriate measures, to ensure that they respect in practice the principles and obligations relating to data processing for employment purposes. At the request of the supervisory authority, employers should be able to demonstrate their compliance with such principles and obligations. These measures should be adapted to the volume and nature of the data processed, the type of activities being undertaken, and should also take into account possible implications for fundamental rights and freedoms of employees.

5. *Collection and storage of data*

5.1. Employers should collect personal data directly from the data subject concerned. When it is necessary and lawful to process data collected from third parties, for example to obtain professional references, the data subject should be duly informed in advance.

5.2. Personal data collected by employers for employment purposes should be relevant and not excessive, bearing in mind the type of the employment as well as the changing information needs of the employer.

5.3. Employers should refrain from requiring or asking an employee or a job applicant access to information that he or she shares with others online, notably through social networking.

5.4. Health data may only be collected for the purposes set out in principle 9 of the present recommendation.

5.5. The storage of personal data for employment purposes is permissible only if the data have been collected in accordance with the requirements outlined in principles 4, 9 and 14 to 20 of this recommendation and only for the time necessary to pursue the legitimate aim of the processing. These data should be relevant, appropriate and not excessive. When evaluation data relating to the performance or potential of an employee are stored, such data should only be used for the purpose of assessing professional skills.

6. *Internal use of data*

6.1. Personal data collected for employment purposes should only be processed by employers for such purposes.

6.2. Employers should adopt data protection policies, rules and/or other instruments on internal use of personal data in compliance with the principles of the present recommendation.

6.3. Under exceptional circumstances, where data are to be processed for employment purposes other than the purpose for which they were originally collected,

employers should take adequate measures to avoid misuse of the data for this different purpose and inform the employee. Where important decisions affecting the employee are to be taken, based on the processing of that data, the employee should be informed accordingly.

6.4. Without prejudice to principle 8, in the event of corporate changes, mergers and acquisitions, particular consideration should be given to the principles of proportionality and purpose specification in the subsequent use of data. Every substantive change in the processing should be communicated to the persons concerned.

7. *Communication of data and use of ICTs for the purpose of employee representation*

7.1. In accordance with domestic law and practice, or the terms of collective agreements, personal data may be communicated to the employee's representatives, but only to the extent that such data are necessary to allow them to properly represent the employee's interests or if such data are necessary for the fulfilment and supervision of obligations laid down in collective agreements.

7.2. In accordance with domestic law and practice, the use of information systems and technologies for the communication of data to employees' representatives should be subject to specific agreements that set out, in advance, transparent rules prescribing their use and safeguards to protect confidential communications, in accordance with principle 10.

8. *External communication of data*

8.1. Personal data collected for employment purposes should only be communicated to public bodies acting in their official functions, and for the purposes of carrying them out, and only within the limits of employers' legal obligations or in accordance with other provisions of domestic law.

8.2. The communication of personal data to public bodies for purposes other than the exercise of their official functions or to parties other than public bodies, including entities in the same group, should only take place:

a. where it is necessary for employment purposes, the purposes are not incompatible with the purposes for which the data was originally collected and if the employee concerned or his or her representatives, as the case may be, are informed of this in advance;

b. with the express, free and informed consent of the employee concerned;

c. if the communication is provided for by domestic law and in particular when necessary for the purpose of discharging legal obligations or in accordance with collective agreements.

8.3. The provisions governing the disclosure of personal data to ensure transparency in the public sector (government and other public authority or body), including monitoring the correct use of public resources and funds, should provide appropriate safeguards for the employee's right to privacy and protection of personal data.

8.4. Employers should take appropriate measures to ensure that only relevant, accurate and up-to-date data are communicated externally, particularly in relation to data that is posted online and accessible to a wider public.

9. *Processing of sensitive data*

9.1. The processing of sensitive data referred to in Article 6 of Convention No. 108 is only permitted in particular cases, where it is indispensable for recruitment to a specific job or to fulfil legal obligations related to the employment contract within the limits laid down by domestic law and in accordance with appropriate safeguards, complementing those set out in Convention No. 108 and in the present recommendation. Appropriate safeguards should be aimed at preventing the risks that the processing of such sensitive data may present to the interests, rights and fundamental freedoms of the employee concerned, notably a risk of discrimination. Processing of biometric data should be possible under conditions provided in Principle 18 of the present recommendation.

9.2. In accordance with domestic law, an employee or a job applicant may only be asked questions concerning his or her state of health and/or be medically examined in order to:

a. indicate his or her suitability for present or future employment;

b. fulfil the requirements of preventive medicine;

c. guarantee an appropriate rehabilitation or comply with any other work environment requirements;

d. safeguard the vital interests of the data subject or other employees and individuals;

e. enable social benefits to be granted;

f. respond to judicial procedures.

9.3. Genetic data cannot be processed, for instance, to determine the professional suitability of an employee or a job applicant, even with the consent of the data subject. The processing of genetic data may only be permitted in exceptional circumstances, for example to avoid any serious prejudice to the health of the data subject or third parties, and only if it is provided for by domestic law and subject to appropriate safeguards.

9.4. Health data and, where their processing is lawful, genetic data, should only be collected from the employee where it is provided for by law, and subject to appropriate safeguards.

9.5. Health data covered by the obligation of medical confidentiality should only be accessible to and processed by personnel who are bound by such an obligation or by other rules of professional secrecy or confidentiality. Such data must:

a. relate directly to the ability of the employee concerned to exercise his or her duties;

b. be necessary in support of measures to protect the health of the employee;

c. be necessary to prevent risks to others.

Where such data are communicated to employers, this processing should be performed by a person with the relevant authorisation, such as someone in personnel administration or responsible for health and safety at work, and the information should only be communicated if it is indispensable for decision making by the personnel administration and in accordance with provisions of domestic law.

9.6. Health data covered by the obligation of medical confidentiality and, where their processing is lawful, genetic data, where appropriate, should be stored separately from other categories of personal data held by employers. Technical and organisational security measures should be taken to prevent persons who do not belong to the employer's medical service having access to the data.

9.7. Health data related to third parties should not be processed under any circumstances unless full, unambiguous, free and informed consent is given by the data subject, or such processing is authorised by a data protection supervisory authority, or it is mandatory according to domestic law.

10. *Transparency of processing*

10.1. Information concerning personal data held by employers should be made available either to the employee concerned directly or through the intermediary of his or her representatives, or brought to his or her notice through other appropriate means.

10.2. Employers should provide employees with the following information:

– the categories of personal data to be processed and a description of the purposes of the processing;

– the recipients, or categories of recipients of the personal data;

– the means employees have of exercising the rights set out in principle 11 of the present recommendation, without prejudice to more favourable ones provided by domestic law or in their legal system;

– any other information necessary to ensure fair and lawful processing.

10.3. A particularly clear and complete description must be provided of the categories of personal data that can be collected by ICTs, including video surveillance and their possible use. This principle also applies to the particular forms of processing provided for in Part II of the appendix to the present recommendation.

10.4. The information should be provided in an accessible format and kept up to date. In any event, such information should be provided before an employee carries out the activity or action concerned, and made readily available through the information systems normally used by the employee.

11. ***Right of access, rectification and to object***

11.1. An employee should be able to obtain, upon request, at reasonable intervals and without excessive delay, confirmation of the processing of personal data relating to him or her. The communication should be in an intelligible form, include all information on the origin of the data, as well as any other information that the controller is required to provide to ensure the transparency of processing, notably information provided in principle 10.

11.2. An employee should be entitled to have personal data relating to him or her rectified, blocked or erased if they are inaccurate and/or if the data have been processed contrary to the law or the principles set out in the present recommendation. He or she should also be entitled to object at any time to the processing of his or her personal data unless the processing is necessary for employment purposes or otherwise provided by law.

11.3. The right of access should also be guaranteed in respect of evaluation data, including where such data relate to assessments of the performance, productivity or capability of the employee when the assessment process has been completed at the latest, without prejudice to the right of defence of employers or third parties involved. Although such data cannot be corrected by the employee, purely subjective assessments should be open to challenge in accordance with domestic law.

11.4. An employee should not be subject to a decision significantly affecting him or her, based solely on an automated processing of data without having his or her views taken into consideration.

11.5. An employee should also be able to obtain, upon request, information on the reasoning underlying the data processing, the results of which are applied to him or her.

11.6. Derogations to the rights referred to in paragraphs 10, 11.1, 11.2, 11.4 and 11.5 may be permitted if provided for by law and are a necessary measure in a democratic society, to protect State security, public safety, important economic and financial interests of the State or the prevention and suppression of criminal offences, the protection of the data subject or the rights and freedoms of others.

11.7. Furthermore, in the case of an internal investigation conducted by an employer, the exercise of the rights referred to in paragraphs 10 and 11.1 to 11.5 may be deferred until the closing of the investigation if the exercise of those rights would prejudice the investigation.

11.8. Unless provisions of domestic law provide otherwise, an employee should be entitled to choose and designate a person to assist him or her in the exercise of his or her right of access, rectification and to object or to exercise these rights on his or her behalf.

11.9. Domestic law should provide a remedy where access to data is refused, or requests for rectification or erasure of any of the data is denied.

12. ***Security of data***

12.1. Employers, or entities which may process data on their behalf, should implement adequate technical and organisational measures in response to periodic reviews of the organisation's risk assessment and security policies and update them as appropriate. Such measures should be designed to ensure the security and confidentiality of personal data processed for employment purposes against accidental

or unauthorised modification, loss or destruction of personal data, as well as against unauthorised access, dissemination or disclosure of such data.

12.2. In accordance with domestic law, employers should ensure adequate data security when using ICTs for any operation of processing of personal data for employment purposes, including their storage.

12.3. The personnel administration, as well as any other person engaged in the processing of the data, should be kept informed of such measures, of the need to respect them and of the need to maintain confidentiality about such measures as well.

13. *Preservation of data*

13.1. Personal data should not be retained by employers for a period longer than is justified by the employment purposes outlined in principle 2 or is required by the interests of a present or former employee.

13.2. Personal data submitted in support of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the job applicant. Where such data are stored with a view to a further job opportunity, the data subject should be informed accordingly and the data should be deleted if he or she so requests.

13.3. Where it is essential to store data submitted for a job application for the purpose of bringing or defending legal actions or any other legitimate purpose, the data should be stored only for the period necessary for the fulfilment of such purpose.

13.4. Personal data processed for the purpose of an internal investigation carried out by employers which has not led to the adoption of negative measures in relation to any employee should be deleted after a reasonable period, without prejudice to the employee's right of access until such deletion takes place.

Part II – Particular forms of processing

14. Use of Internet and electronic communications in the workplace

14.1. Employers should avoid unjustifiable and unreasonable interferences with employees' right to private life. This principle extends to all technical devices and ICTs used by an employee. The persons concerned should be properly and periodically informed in application of a clear privacy policy, in accordance with principle 10 of the present recommendation. The information provided should be kept up to date and should include the purpose of the processing, the preservation or back-up period of traffic data and the archiving of professional electronic communications.

14.2. In particular, in the event of processing of personal data relating to Internet or Intranet pages accessed by the employee, preference should be given to the adoption of preventive measures, such as the use of filters which prevent particular operations, and to the grading of possible monitoring on personal data, giving preference for non-individual random checks on data which are anonymous or in some way aggregated.

14.3. Access by employers to the professional electronic communications of their employees who have been informed in advance of the existence of that possibility can only occur, where necessary, for security or other legitimate reasons. In case of absent employees, employers should take the necessary measures and foresee the appropriate procedures aimed at enabling access to professional electronic communications only when such access is of professional necessity. Access should be undertaken in the least intrusive way possible and only after having informed the employees concerned.

14.4. The content, sending and receiving of private electronic communications at work should not be monitored under any circumstances.

14.5. On an employee's departure from an organisation, the employer should take the necessary organisational and technical measures to automatically deactivate the employee's electronic messaging account. If employers need to recover the contents of an employee's account for the efficient running of the organisation, they should do so before his or her departure and, when feasible, in his or her presence.

15. *Information systems and technologies for the monitoring of employees, including video surveillance*

15.1. The introduction and use of information systems and technologies for the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted. Where their introduction and use for other legitimate purposes, such as to protect production, health and safety or to ensure the efficient running of an organisation has for indirect consequence the possibility of monitoring employees' activity, it should be subject to the additional safeguards set out in principle 21, in particular the consultation of employees' representatives.

15.2. Information systems and technologies that indirectly monitor employees' activities and behaviour should be specifically designed and located so as not to undermine their fundamental rights. The use of video surveillance for monitoring locations that are part of the most personal area of life of employees is not permitted in any situation.

15.3. In the event of dispute or legal proceedings, employees should be able to obtain copies of any recordings made, when appropriate and in accordance with domestic law. The storage of recordings should be subject to a time limit.

16. Equipment revealing employees' location

16.1. Equipment revealing employees' location should be introduced only if it proves necessary to achieve the legitimate purpose pursued by employers and their use should not lead to continuous monitoring of employees. Notably, monitoring should not be the main purpose, but only an indirect consequence of an action needed to protect production, health and safety or to ensure the efficient running of an organisation. Given the potential to violate the rights and freedoms of persons concerned by the use of these devices, employers should ensure all necessary safeguards for the employees' right to privacy and protection of personal data, including the additional safeguards provided for in principle 21. In accordance with principles 4 and 5, employers should pay special attention to the purpose for which such devices are used and to the principles of minimisation and proportionality.

16.2. Employers should apply appropriate internal procedures relating to the processing of these data and should notify the persons concerned in advance about them.

17. Internal reporting mechanism

17.1. Where employers are obliged by law or internal rules to implement internal reporting mechanisms, such as hotlines, they should secure the protection of personal data of all parties involved. In particular, employers should ensure the confidentiality of the employee who reports on illegal or unethical conduct (such as whistleblowers). Personal data of the parties involved should be used solely for the purpose of appropriate internal procedures relating to the report and as required by law, or as may be required for subsequent judicial proceedings.

17.2. Under exceptional circumstances, employers may enable anonymous reporting. Internal investigations should not be carried out on the sole basis of an anonymous report, except where it is duly circumstantiated and relates to serious infringements of domestic law.

18. Biometric data

18.1. The collection and further processing of biometric data should only be undertaken when it is necessary to protect the legitimate interests of employers, employees or third parties, only if there are no other less intrusive means available and only if accompanied by appropriate safeguards, including the additional safeguards provided for in principle 21.

18.2. The processing of biometric data should be based on scientifically recognised methods and should be subject to the requirements of strict security and proportionality.

19. Psychological tests, analysis and similar procedures

19.1. Recourse to psychological tests, analysis and similar procedures performed by specialised professionals, subject to medical confidentiality, that are designed to assess the character or personality of an employee or a job applicant should only be allowed if legitimate and necessary for the type of activity performed in the job and if domestic law provides appropriate safeguards.

19.2. The employee or the job applicant should be informed in advance of the use that will be made of the results of these tests, analysis or similar procedures and, subsequently, the content thereof. Principles 11.1 and 11.2 apply accordingly.

20. Other processing posing specific risks to employees' rights

20.1. Employers or, where applicable, processors, should carry out a risk analysis of the potential impact of any intended data-processing on the employees' rights and fundamental freedoms and design data processing operations in such a way as to prevent or at least minimise the risk of interference with those rights and fundamental freedoms.

20.2. Unless domestic law or practice provides other appropriate safeguards, the agreement of employees' representatives should be sought before the introduction or adaptation of ICTs where the analysis reveals risks of interference with employees' rights and fundamental freedoms.

21. ***Additional safeguards***

For all particular forms of processing, set out in Part II of the present recommendation, employers should ensure the respect of the following safeguards in particular:

a. inform employees before the introduction of information systems and technologies enabling the monitoring of their activities. The information provided should be kept up to date and should take into account principle 10 of the present recommendation. The information should include the purpose of the operation, the preservation or back-up period, as well as the existence or not of the rights of access and rectification and how those rights may be exercised;

b. take appropriate internal measures relating to the processing of that data and notify employees in advance;

c. consult employees' representatives in accordance with domestic law or practice, before any monitoring system can be introduced or in circumstances where such monitoring may change. Where the consultation procedure reveals a possibility of infringement of employees' right to respect for privacy and human dignity, the agreement of employees' representatives should be obtained;

d. consult, in accordance with domestic law, the national supervisory authority on the processing of personal data.

COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Ministers' Deputies
CM Documents

CM(2015)32 addfinal 1 April 2015[1]

1224 Meeting, 1 April 2015

5 Media

5.1 Steering Committee on Media and Information Society (CDMSI)

a. Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment – Explanatory Memorandum

EXPLANATORY MEMORANDUM

to Recommendation CM/Rec(2015)5
of the Committee of Ministers to member States
on the processing of personal data in the context of employment

(Adopted by the Committee of Ministers on 1 April 2015
at the 1224th meeting of the Ministers' Deputies)

Introduction

1. Recommendation No. R (89) 2 of the Committee of Ministers to member States on the protection of personal data used for employment purposes was the sixth such instrument adopted by the Committee of Ministers within the framework of the "sectoral approach" to data protection issues.

2. Twenty-five years have passed since the recommendation was adopted. Work per se has changed a lot (in terms of subject matter, form, duration and intermediaries), as have the places where it is performed and the way in which it is organised. Employers, employees and their needs have changed, and due to the increasing use of new technologies, the spectrum of personal data that is handled has become broader (IP addresses, log files and location data, for example). The need to review the recommendation thus became clear.

3. The Consultative Committee of Convention 108 mandated an expert in 2011 to carry out a study on Recommendation No. R (89) 2 and to suggest proposals for its revision (document T-PD-BUR(2010)1FIN – "Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes – proposals for the revision of the above-mentioned Recommendation" by Giovanni Buttarelli).

4. On the basis of the study, the consultative committee worked on the revision of the recommendation and approved the draft text during its 31st Plenary meeting (2-4 June 2014). It subsequently transmitted the draft revised recommendation to the Steering Committee on Media and Information Society (CDMSI) for examination and approval, which ensured parallel consultation of the European Committee on Legal Co-operation (CDCJ).

5. With regard to the development of context as compared to 1989, the following elements were taken into consideration:

- the growing use of information technologies in the context of employment and the need to protect employee's dignity and fundamental rights against the monitoring of their activities;
- the tendency of employers to collect data on employees outside the strict perimeter of work, as for example on search engines and social networking sites;

[1] This document has been classified restricted until examination by the Committee of Ministers.

- the introduction of particular forms of processing carrying specific risks to individuals, involving for instance biometric or location data.

6. The draft recommendation was approved by the CDMSI at its 7th meeting (18-21 November 2014).

7. The Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment was adopted by the Committee of Ministers of the Council of Europe on 1 April 2015.

Preamble

8. The preamble sets out the reasons that have led the Committee of Ministers to present the recommendation to governments of member States.

9. The work of the Council of Europe in the field of data protection has always supported the position that information systems and technologies (ICTs) bring undoubted benefits to society. The main concern of the Organisation in this area has been to set standards allowing technological progress to be accompanied by a clear recognition of the need to safeguard the interests of the individual, in particular in respect of data processing.

10. The employment sector, private and public – to which the principles contained in this recommendation are directed – reflects this preoccupation: how to strike a balance between the undoubted advantages offered by technology to enterprises on the one hand and on the other, the rights and freedoms of employees in a work environment where ICTs are part of the employees' daily activities. The benefits which result for them in better organisation of work, a reduction in routine tasks and so on, must be evaluated in the light of the possible impact on the privacy of the individual employee, and of the workforce of an entity as a whole, which technology may possibly produce. The preamble also recognises that other rights and freedoms may possibly be put at risk through the introduction of ICTs in the workplace – for example, freedom of association or freedom of expression as guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5, more commonly known as the European Convention on Human Rights and hereinafter "ECHR"), as well as the rights guaranteed by the European Social Charter which are of direct concern to the relationship between employers and employees.

11. The first paragraph of Article 8 of the ECHR provides that "Everyone has the right to respect for his private and family life, his home and his correspondence". The European Court of Human Rights (hereinafter "the Court") has also developed case law under which Article 8 may also give rise to positive obligations that are inherent to the effective "respect" for private life. In light of those positive obligations, the State must take the necessary measures, including legislative ones, to ensure in practice effective compliance with the rights deriving from Article 8 of the ECHR.

12. At the outset, the point is made that privacy is not simply to be interpreted in terms of the right of the employee to be free from unjustified intrusion into his or her workaday life, although the recommendation's principles on monitoring and surveillance of employees are closely related to this traditional meaning of the concept of privacy. Rather, the principles set out reflect the concern spelt out in the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) of 28 January 1981 (hereinafter referred to as "Convention 108") to protect the data subject through the regulation of the processing (collection, use, storage, etc.) of personal information.

13. The recommendation is, accordingly, structured in such a way as to make Convention 108's broad principles meaningful to the employment context by offering principles designed to regulate the relevant activities of the employer. In other words, by adapting the convention's basic principles relating to fair and lawful processing, intended purposes, proportionality, data minimisation and access to data, the guidelines set out in the recommendation provide responses to questions such as: how should data be collected by employers? For what purposes? What use can be made of the data stored? What are the rights of the employee in regard to the data processed by the employer?

14. Given that the recommendation constitutes a sectoral approach to data protection, it is necessary to take into account all the elements distinguishing the sector in question and which influence the way in which Convention 108's basic principles are to be adapted. Accordingly, the text seeks to reflect the typical legitimate information needs of the employer as well as the legitimate privacy/data protection needs of the employee. However, and as the preamble points out, it is also a feature of the employment sector that both group interests and individual interests are at stake. A valid sectoral approach must also seek to tailor Convention 108's broad principles to the reality of the collective interest. It is for this reason that, at various stages in the text, the principles set out in the recommendation accept the possibility of employee

representatives defending the data protection interests of the individual employee and employees as a whole within an entity.

15. As regards the implementation of the recommendation's principles, governments of member States should ensure that the principles contained in the appendix of the recommendation are reflected in the application of domestic legislation on data protection in the employment sector, as well as in other branches of the law which have a bearing on the use of personal data for employment purposes.

16. The purview of the recommendation allows for a number of ways in which these principles can be implemented. In the first instance, it is possible for the data protection authorities established pursuant to the national data protection legislation to avail themselves of the principles when they are confronted by problems of data protection in the context of employer-employee relations. The governments of the member States should, accordingly, ensure that such authorities are aware of the existence of the recommendation and of its value to dispute resolution in this sector. Convention 108, to which the domestic norms conform, makes no exception for the employment sector. Accordingly, national data protection authorities responsible for the application of the domestic norms can usefully avail themselves of the provisions of the recommendation to help them discharge their tasks in giving effect to data protection norms in the employment sector. By way of example, the principles could be used by them in specific cases or as a basis for proposed codes of conduct in the employment field. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, which lays down rules regulating the processing of personal data in profiling techniques, can be of particular relevance in the context of employment.

17. Beyond these considerations, it is felt that social partners themselves can negotiate acceptance and respect for the principles, either as a complement to the existing legal regulations or as an alternative to it. The preamble takes into account the different national approaches to government involvement in labour relations, which may range from varying degrees of regulation to free collective bargaining - free from State intervention - between the social partners on issues relating to employer-employee relations. Accordingly, in the absence of legislative initiatives designed to give effect to the principles of the recommendation, governments should ensure that the representative bodies of employers and employees are adequately informed of the value of the recommendation's approach to data protection issues.

Appendix to Recommendation CM/Rec(2015)5

Part I - General principles

1. Scope

18. Consistent with the scope of Convention 108, the principles contained in the recommendation apply to the processing of personal data in public and private sector employment. As will be seen hereafter, "employment purposes" is to be understood as covering a range of processing activities relating to recruitment, performance of the contract of employment, discharge of obligations laid down by law or laid down in collective agreements, the management planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of termination of the employment relationship.

19. Principle 1.2 of the recommendation brings the activities of employment agencies or "head-hunting agencies" in the public and private sectors within the scope of some of its provisions ("unless domestic law provides otherwise"). It may be the case that a number of member States consider public sector employment agencies in a different context to the employment field and regulate them outside the scope of labour law – for example by social security law. While such countries may decide not to apply the principles of the recommendation to their activities, it will nevertheless be the case that general data protection legislation of the countries in question will apply to their data processing activities.

20. According to Principle 1.2, employment agencies shall use the data in their capacity either as data controllers or as processors, in compliance with the principles of this recommendation and only for the purposes for which the data were initially collected. In some cases, employment agencies shall use the data of candidates to help employers discharge their duties relating to the contracts of employment.

2. Definitions

21. The definition of "personal data" is consistent with that of Convention 108. It is a long-lasting established definition which has been reaffirmed over the years through a variety of legal instruments of the

Council of Europe. The term “personal data” is defined broadly and should be interpreted in such a way as to allow it to also respond to the increasing use of new technologies and means of electronic communication in the relations between employers and employees. Personal data may include an employee’s name, age, home address, marital status, education, log files, etc. It may also include an employer’s appraisal or opinion of an employee and a digitised image of the employee.

22. The definition of “personal data” refers to any information relating to an identified or an identifiable person. “Identifiable individual” means a person who can be directly or indirectly identified. An individual is not considered “identifiable” if his or her identification would require unreasonable time, effort or means. The determination of what constitutes “unreasonable time, effort or means” should be assessed on a case-by-case basis, in the light of the purpose of the data processing and taking into account objective criteria such as the cost, in relation to the benefits, of such an identification, the technology used and available at the time of the processing, technological developments, etc.

23. Data that appears to be anonymous because it is not accompanied by any obvious identifiers may nevertheless, in particular cases, permit the identification of the individual concerned. This is the case where, for example, alone or through the combination of physical, physiological, genetic, mental, economic, cultural or social data (such as age, sex, occupation, geolocation, family status, etc.), it is possible for the controller, or any legitimate or illegitimate actor (in particular when the data was made publicly available) to identify the person concerned. Where this is the case, the data may not be considered to be anonymous and must therefore be treated as personal data.

24. “Data processing” covers an open-ended general notion capable of flexible interpretation which starts from the collection or creation of personal data and covers all automated operations, whether partially or totally automated. Data processing also occurs where no automated operation is performed but data are organised in a structure which allows a search, combination or correlation of the data related to a specific employee or potential employee.

25. “Information systems” refers to any kind of devices such as computers, cameras, video equipment, sound devices, telephones and other communication equipment, as well as various methods of establishing identity and location, or any method of surveillance. The terms “tools” and “devices” are covered by the notion of “information systems” and information technologies, whose definitions are outlined in the recommendation.

26. As regards the notion of “employment purposes”, it should be emphasised that the principle of purpose or purpose specification is of crucial importance, serving as it does to define and limit the personal information activities of the employer. As provided for in Convention 108, personal data undergoing processing should be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes. The purpose identified for this sector – "employment purposes" – seeks to balance the interests of the employer with those of the employees while, at the same time, accepting that the employer may act as intermediary between the State and the employee for the purpose of collecting and storing personal data for subsequent transmission to the State; for example, when it is pursuant to tax or social security or industrial safety legislation ("the discharge of obligations laid down by law").

27. “Employment purposes” shall also cover the disciplinary framework (e.g. internal investigations and sanctions), as well as data processed after the termination of employment. It should be clarified that when the data are stored after the termination of employment, the processing should be in line with Principle 13 and with the principle of intended purpose. The term “contract of employment” should be understood as an oral or written, expressed or implied, agreement, specifying terms and conditions under which a person consents to perform certain duties as directed and controlled by an employer, usually but not always in return for a previously agreed wage or salary. It was understood that for the drafters of the recommendation the term “contract of employment” would also refer to non-remunerated employment such as volunteering jobs, internships and training courses. The principles of the recommendation thus also apply to individuals who are in an employment relationship with such status. Furthermore, the employment relationship in the public sector should be covered, even if it is not necessarily based on a contract of employment. The employment terms, conditions and duties are usually specified under the relevant regulations of administrative law.

28. The “employer” is a legal entity that controls and directs an employee in the context of an employment relationship, which generally exists when a person performs work or services under certain conditions in return for remuneration. It is through the employment relationship that reciprocal rights and obligations are created between the employee and the employer. It has been, and continues to be, the main vehicle through which workers gain access to the rights and benefits associated with employment in the areas of labour law and social security.[2]

[2] Source ILO: www.ilo.org/ifpdial/areas-of-work/labour-law/WCMS_CON_TXT_IFPDIAL_EMPREL_EN/lang--en/index.htm.

29. An “employee” is a person who is hired to perform work for an employer within an employment relationship. The terms of “worker” or “staff member” also refer to the definition of “employee”. Special attention should be given to the concept of employee and, in this regard, to the ruling of the Court of Justice of the European Union (CJEU) in the Case C-94/07 – *Andrea Raccanelli v. Max-Planck-Gesellschaft zur Förderung der Wissenschaften eV*. The CJEU ruled that the concept of the “worker” within the meaning of Article 35 of the Treaty on the Functioning of the European Union (TFEU) has a specific meaning in EU law and must not be interpreted narrowly. Any person who pursues activities which are real and genuine, to the exclusion of activities of such a small scale as to be regarded as purely marginal and ancillary, must be regarded as a “worker”. The essential feature of an employment relationship is that, according to this case law, for a certain period of time a person performs services for and under the direction of another person in return for which he or she typically receives remuneration.

30. Prospective employees should benefit from the same protection and rights as employees, even if their candidature does not lead to a contract of employment. Similarly, it should be underlined that the principles of this recommendation also apply to former employees.

3. Respect for human rights, human dignity and fundamental freedoms

31. Principle 3 constitutes a general statement which informs the approach taken in the rest of the recommendation to the issue of personal data processing in the employment field. Privacy is to be seen in terms of data protection and as imposing limits on the processing of personal information by employers. In this sense, it is also to be seen as conferring positive rights on employees to allow them to make sure, through the rights specified in Principle 11, that employers have respected the requirements of data protection.

32. The reference to “human dignity” in the text takes account of the fact that technology should not be used in a way which inhibits social interaction among employees. These concerns are reflected later in the text.

33. The approach taken is consistent with the position adopted by the European Court of Human Rights, which has stated repeatedly that it is difficult to completely separate matters of private and professional life. In *Niemietz v. Germany*,[3] which concerned the search by a government authority of the complainant’s office, the Court held that Article 8 afforded protection against the search of someone’s office by stating: "Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of ‘private life’ should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world. This view is supported by the fact that, as was rightly pointed out by the Commission, it is not always possible to distinguish clearly which of an individual’s activities form part of his professional or business life and which do not”.

34. Moreover, in the case of *Halford v. the United Kingdom*,[4] the Court decided that interception of workers’ phone calls at work constituted a violation of Article 8 of the Convention, ruling that “telephone calls made from business premises as well as from the home may be covered by the notions of ‘private life’ and ‘correspondence’ within the meaning of Article 8 paragraph 1 (…)”.

35. In *Copland v. the United Kingdom*,[5] the Court reaffirmed this position in respect of the monitoring of an employee’s use of telephone, e-mail and the Internet. The Court considered that the collection and storage of personal information relating to Ms Copland through her use of the telephone, e-mail and Internet interfered with her right to respect for her private life and correspondence, and that that interference was not “in accordance with the law”, there having been no domestic law at the relevant time to regulate monitoring. While the Court accepted that it might sometimes have been legitimate for an employer to monitor and control an employee’s use of telephone and Internet, in this case it was not required to determine whether that interference was “necessary in a democratic society”.

4. Application of personal data protection principles

36. Information systems and technologies used for the processing of personal data in the context of employment should be used in such a way as to minimise the processing of personal data, as well as to limit

[3] *Niemietz v. Germany*, Application No. 13710/88, 16 December 1992.
[4] *Halford v. the United Kingdom*, Application No. 20605/92, 25 June 1997.
[5] *Copland v. the United Kingdom*, Application No. 62617/00, 3 April 2007.

the use of data identifying or allowing the identification of individuals to only that necessary for the aims pursued in the individual cases concerned.

37. Principle 4.2 states that employers should develop appropriate measures to ensure that they respect in practice the principles and obligations relating to data processing for employment purposes and that they should furthermore be in a position to demonstrate their compliance with such principles to the relevant supervisory authority. According to this principle, employers are obliged to put in place measures aimed at guaranteeing that data protection rules are adhered to in the context of processing operations and to maintain records of categories of personal data processing activities under their responsibility, in order to prove to employees and to supervisory authorities that measures have been taken to achieve compliance with the data protection rules.

38. It must also be stressed that data protection principles should also be respected in both the development and the use of technologies and that the principles of Convention 108 are fully applicable in this regard (notably those relating to the quality of data, sensitive data, data security and the rights of the data subjects). Experience has shown that in the context of employment, the employer will seek to efficiently manage his business and optimise the use of new technologies and thus benefit from their potential. Hence, these new technologies, such as video surveillance, biometrics or geolocation, give the employer the opportunity to monitor all activities of employees, if the law does not regulate or prohibit such monitoring. The manner in which the data protection principles should be respected and how to strike a balance between the employees' rights and any legitimate interest of the employer will be developed later in the text.

39. Moreover, according to Principle 4.2, the measures should be adapted to the volume and nature of data processed, as well as the scope, context and purpose of the processing and, in respect of this, appropriate simplified solutions should be adopted in small-scale working environments. The recommendation does not make a distinction between small or medium-sized and large working environments for the purpose of the application of the recommendation's principles. It is felt that the size of the working environment is not a decisive factor for data protection since problems may arise regardless of the number of people employed by an employer. The principles can be readily applied by small working environments, including small family businesses, with a minimum of requirements. However, legislation should be sensitive to the need not to impose unnecessary legal requirements on small working environments which process small volumes of non-sensitive data.

5. Collection and storage of data

40. Principle 5 seeks to adapt some of the protective provisions within Article 5 of Convention 108 to the collection of data concerning individuals by their employers. The principle is not restricted solely to data collection on employees within the course of their employment. It also addresses the data protection needs of job applicants, even if no employment offer has been made to them. It is felt desirable to also provide guidelines relating to data collection at the recruitment stage.

41. Principle 5.1 emphasises the need to make the individual employee the primary source of information. In other words, if the employer requires information on a named employee, then such information should be sought directly from the employee. This is not an absolute rule. The text of Principle 5.1 accepts that it may be necessary at times to bypass the individual employee so as to obtain data on him or her, for example, to check the accuracy of information supplied by a prospective employee in the course of a hiring or promotion procedure, on condition that the employee, or prospective employee, has been duly informed before the data is collected from third parties.

42. It is important to stress in the context of Principle 5 that many aspects of the processing of employees' data do not require specific consent, as they have another legitimate basis prescribed by law. There are limitations as to how far consent can be relied upon in the employment context to justify the processing of personal data. To be valid, consent must be informed, "freely given" and limited to cases where the employee has a genuinely free choice and is subsequently able to refuse or withdraw consent without detriment. In general, all data processing within the context of employment should be provided for by domestic law.

43. It emerges from Principle 5.2 that the amount of personal information which can be legitimately collected on employees depends on the job in question. Employers should review their data collection practices – for example, the type of data required on application forms – so as to ensure that they are not storing more personal information than necessary in view of the nature of the employment or the needs of the moment. The text accepts that, at certain periods in the life of an entity, it may be necessary for the employer to obtain more data than normal – for example, for the purposes of a proposed merger or wholesale restructuring, it may be appropriate to seek the personal views of the employees. Here it may be noted that in

addition to the requirements of relevancy and accuracy, the collection procedure must also respect the principle of proportionality and transparent and fair processing.

44. Using search engines for instance to assemble data (including sounds, pictures or videos) can have a significant impact on a person's private and social life, especially if personal data derived from a search is incomplete, excessive, incorrect or not relevant any more. A preventive approach inspired by a rationale of privacy by design could reduce implementing problems, by encouraging the distribution of privacy-oriented products which are more focused, from a technical and organisational viewpoint, on the principles of necessity, data minimisation and proportionality.

45. Principle 5.3 refers to the concept of "social networking". A social networking service is a platform which enables the building of social relations among people who share interests, activities, backgrounds or real-life connections. It is a web-based service that allows individuals to create a profile, to establish a list of users with whom to share views and to develop contacts within the system. Controllers of social networking services are themselves bound to the principles of data protection and to the correspondent obligations, especially in terms of information, violations of terms of service and proportionality. However, employers should refrain from collecting data relating to job applicants or employees without their knowledge through an intermediary, under another name or using a pseudonym.

46. When an employee's or prospective employee's access to social networking accounts is restricted, employers do not have the right to ask for access to such accounts, for instance by requiring that employees/prospective employees provide them with their login credentials.

47. Although the collection and processing of health data is dealt with under Principle 9, the drafters of the recommendation considered it to be important to recall this rule in Principle 5.4, given that health data are sensitive data and their processing in the employment context can only occur where appropriate safeguards are put in place and specific conditions met.

48. The storage of personal data referred to in Principle 5.5 is linked to the collection of data. Employers should have a legitimate grounds for storing the personal data of employees that have been collected for employment purposes, and the length of the storage period will depend on the need for and the purpose of the processing. To this end, data collected on job applications and interview records of candidates that have not been accepted should be stored for a very short period (see also paragraphs 107-108).

6. Internal use of data

49. Principle 6 deals solely with the situation where personal data are used internally by the employer. Principle 6.1 underlines the need to respect the purposes specification. Personal data collected and stored for employment purposes should only be used for those purposes. It is important to identify clearly the various circumstances in which personal data can be legitimately used for "employment purposes" and to provide the necessary specifications and safeguards. However, it should be borne in mind that the expression "employment purposes" covers a range of sub-purposes for which data can be processed. For example, personal data may be processed for the purpose of administering an employee training scheme, or a company loan or pension scheme, or the data may relate to candidates who have put themselves forward for promotion, or they may be processed for salary purposes. It is important to consider the context for which the data were collected, since random use of data, although for an employment purpose, may distort the purpose for which data were originally collected.

50. With due regard to the principles of relevance and accuracy, and with regard in particular to large-scale or territorially extensive working environments, certain personal data, for example e-mail addresses or pictures, could be made easily accessible in internal communication networks in order to speed up the performance of the work carried out and to facilitate interaction with other employees. In such cases employees concerned should be duly informed about the internal communication of their data.

51. Principle 6.2 encourages employers to adopt internal privacy policies/rules and to inform employees about them. Such rules should take account of the data protection principles outlined in the recommendation and, more specifically:

- the principle of fair processing: data collection directly from the employee concerned, information provided to the employees, the exercise of the employee's rights;
- the purpose of the processing: data should be collected for explicit, legitimate and specified purposes and should not be used for other purposes;
- the communication of data: only for the purposes provided above;

- data security: appropriate security measures should be provided to prevent unauthorised access to, or alteration, disclosure or destruction of, the data and to prevent their accidental loss or destruction;
- measures on how to keep data accurate and up to date: in order to prevent taking decisions or actions based on inaccurate data;
- the limitations on data storage: this requirement places a responsibility on employer to be clear about the length of time for which data will be kept and the reason for retaining the information;
- the rights of employees;
- the obligations of the employer.

52. Employers are further encouraged to adopt binding internal procedures and/or policies defined prior to the introduction of new data processing operations; for example, how to provide adequate information to employees or how to give them adequate replies in the event that they exercise their rights or complain.

53. Principle 6.3 recommends the taking of adequate measures so as to guarantee that the new context in which data are redeployed reflects faithfully the original contextual meaning assigned to the data as well as continuing respect for the specific purpose for which the data were collected and stored. For example, when an employer is considering whether or not an employee's wages should be reduced for repeated absence or irregular attendance, care should be taken to analyse attendance data to ensure that the employee is not absent because of his or her attendance on an authorised training scheme. Alternatively, the fact that an employee's file reveals that his or her repayments of a company loan are in arrears should not be taken into consideration in the context of disciplinary proceedings.

54. Moreover, irrespective of different national approaches to the issue of "incompatibility", it may also be the case that an employer's undertaking that he or she will not use data collected for certain purposes for other purposes within the employment relationship may effectively restrict subsequent use of the data. Sometimes the very nature of the original purpose for which personal data were collected – for example statistics or research relating to industrial diseases – will preclude the subsequent use of the data collected for another unrelated employment purpose. Whether or not subsequent use of personal data is to be considered "incompatible" with the original purpose for which the data were collected is to be assessed on a case-by-case basis.

55. Informing the employee of any proposed use of data drawn from different contexts in order to take decisions which affect his or her interests is seen as a safeguard for the employee against the sort of prejudice illustrated above. This is a fundamental requirement of the principle of fair processing and of transparency which governs the employment relationship.

56. In the event of the transfer of undertakings or businesses, it may be acceptable that certain categories of employees' personal data be communicated to third parties (e.g. to other companies of the same group or to the new employer in the event of acquisitions or mergers, transfer of contracts, etc.). The amount of personal information on employees which can be legitimately communicated to third parties will of course depend on the job in question and, in addition to the requirements of relevancy and proportionality, the communication will also be linked to respect for the purposes specification ("for employment purposes"). Where substantive changes in the processing occur, the persons concerned should also be informed in due respect of applicable law and as may be found appropriate by data protection authorities. Where the transfers of undertakings or businesses result in a transfer of employees' data to third countries, those can only take place where the third country ensures an adequate level of protection for the data or appropriate safeguards.

57. The text of Principle 6 says nothing about the issue of the processing of personal data for research or statistical purposes by employers. Planning and organisation of work may require this to be carried out at times. Should this be the case, the principles laid down in Recommendation No. R (83) 10 on the protection of personal data used for scientific research and statistics should be respected.

7. Communication of data and use of ICTs for the purpose of employee representation

58. The meaning to be assigned to the term "employee's representatives" will be determined by national law and practice in the field of labour relations. These representatives may include works councils, trade union representatives or other associations to which the employee is affiliated. The names and addresses of employees may in some cases need to be communicated to the representative organ so as to allow literature relating to proposed union elections to be circulated. The communication of personal data relating to employees who are not affiliate to a representative body should be done with their consent. However, if the purpose is to verify compliance with a collective agreement or other terms of employment and this is made through employee's representatives, which may be the case for some member States, transfer of personal data relating to employees who are not members of the representative body can be done if necessary to verify such compliance.

59. The term “collective agreement” should be understood as an agreement between an employers’ organisation or an employer, on the one hand, and a trade union on the other. The agreement should be in writing and should normally detail the conditions of employment and the relationship between the employer and the employee.

60. Furthermore, for the purposes of this recommendation, the term “communication” provided for in Principles 7 and 8 should include the disclosure, transmission and transfer of personal data.

61. The quantity of personal information which can be communicated should satisfy the principle of proportionality – only that that is "necessary to allow them [the representatives] to represent the interests of the employees". The particular national context will obviously influence the amount of data which can be communicated to representative bodies, in particular the existence of statutory regulations on the relations between employers and representative bodies. For example, national law may authorise the communication of personal data relating to a candidate for promotion so as to allow a works council to be consulted before any decision is taken. The obligations provided in collective agreements, stated in the Principle 7.1, usually concern both employers and employees and may refer for instance to pay agreements, employment conditions and joint dispute resolution procedures.

62. Information systems referred to in Principle 7.2 are those defined in Principle 2. New technologies, such as e-mails or intranet, may be used for the communication of employees’ data to their representatives. This communication should be done in accordance with domestic law and practice. The agreements setting the procedures for the secure use of the data and the confidentiality of the communications should also be provided for in domestic law or determined by the data protection authorities.

63. Reference could be made here to electronic voting, often online, which has been increasingly developed during recent years, particularly for employees’ representatives elections within companies. Electronic voting operations may pose risks to employees, notably the risk of disclosure of sensitive data such as trade union membership or political opinions. The processing of personal data necessary for elections should seek to ensure the protection of the privacy of employees. The implementation of effective security measures is essential for a successful vote operation, such as the use of cryptographic methods, sealing and encryption.

64. The data processed by representative bodies in these circumstances are naturally subject to the general principles of data protection, particularly so in the case of electronic voting referred to above.

8. External communication of data

65. It has been noted that the employer may act as an intermediary between the State and the employee for the purpose of supplying data to State agencies, such as those referred to in Principle 8.1. It may for instance be tax or social security authorities or health and safety inspectorates. The nature and amount of personal data which can be communicated to such public bodies or State agencies will be determined by the level of fulfilment of the statutory duties. "Legal obligations" should be understood in this sense.

66. Public bodies may require the processing of personal data to enable them to exercise their official functions – for example, government research in the field of job-related injuries and diseases or the analysis of employment patterns in deprived areas. It is accepted that the expression “in accordance with other provisions of domestic law” may oblige communication of employee data in those circumstances (for the definition of “communication” see paragraph 56 above) and will depend on the national context. In addition, domestic law, in compliance with the ECHR, may at various times require the communication of personal data to the police, courts and other public bodies discharging official functions. It will be noted that, in these cases, personal data are not being communicated for employment purposes. For example, divorce proceedings involving an employee and his/her spouse may require the communication of data relating to his/her salary by the employer to the court so as to enable it to assess the amount of maintenance which should be paid on the dissolution of their marriage. Regarding the communication of personal data to the police – which may be required by domestic law as applied in conformity with Convention 108 – reference should also be made to the provisions of Recommendation No. R (87) 15 of the Committee of Ministers to member States regulating the use of personal data in the police sector.

67. Principle 8.2 addresses the situation where personal data are to be communicated outside the place of employment to public bodies not exercising official functions – for example a government agency acting as employer in the labour market – and to private parties, including entities within the same group.

68. Principle 8.2.*a* deals with the communication of personal data for employment purposes to the type of bodies referred to above. For example, an employer may engage an auditor to run the company accounts, pay wages, deal with personal tax liability of employees, etc. Or an employee may be on a temporary assignment with another employer. Both examples will require the disclosure of personal data. The text accepts that communication in such circumstances is legitimate since the sort of matters referred to fall within the scope of the expression "employment purposes". It should be noted that the legitimacy of communication in those circumstances is made subject to ensuring respect for purposes specification ("which are not incompatible with the purposes for which the data were originally collected") and the considerations discussed under Principle 6.3 are equally valid for the interpretation of Principle 8.2.*a*. Principle 8.2.*a* also makes communication of the data conditional on prior information being given to the employee concerned or his/her representatives. Once again, the text of the recommendation recognises the value of data protection operating in conjunction with transparency.

69. As regards Principle 8.2.*b*, the personal data to be communicated may not be intended for use for employment purposes – for example, a request made by a direct marketing firm or a political party to have lists of employees' names and addresses. In situations such as these, the safeguards are increased: the express, freely given, specific and informed consent of the individual employee must be obtained.

70. It may also be the case that domestic law authorises the communication of personal data to private bodies or public bodies not discharging official functions. National legislation on statistics may be such a case. More often, the communication referred to in Principle 8.2.*c* is provided for the purpose of discharging legal obligations, relating for example to social security and the welfare of employees, or to optimise the allocation of human resources or, where necessary, for judicial purposes, including the exercise of the right to remedy.

71. Principles 8.3 and 8.4 were introduced in the light of other legislation that aims to enhance the transparency of public administrative activities and to facilitate access to public records by introducing various obligations for public administrative bodies to publish and disseminate records, documents and information on their organisation and activities. Communication of data relating to a public authority's staff can cover a wide range of topics, including the names of employees, organisation charts and internal directories, as well as other data where individual employees can be identified, such as information on salaries and pensions, severance payments and compromise agreements, sickness statistics and training records.

72. There are a number of factors that could indicate whether communication would be fair, including whether it is necessary and proportional to the fulfilment of the public interest, if it is sensitive personal data, the consequences of disclosure and the balance between the employees' rights and any legitimate public interest in disclosure. In principle, the information should relate to their public role rather than their private life. When it comes to sensitive personal data, full respect of Article 6 of Convention 108 should be ensured. These data are likely to relate to the most personal aspects of employees' lives, for example their health or sexual life, rather than their working life.

73. Additional safeguards may be considered for the fair processing and publication of employees' data, such as the determination of proportionate time limits for their publication as well as taking measures for restricting the availability of such information on external search engines.

9. Processing of sensitive data

74. As with Convention 108 and other recommendations in the field of data protection, a separate principle is devoted to the issue of sensitive data. It will be noted however that Principle 9 also lays down special guidelines for the processing of health data, given that such data are a more common feature of the employment sector than the other types of data referred to in Principle 9.1. For this reason, health data require more extensive consideration. Due attention should also be paid to Recommendation No. R (97) 5 of the Committee of Ministers to member States on the protection of medical data.

75. Particular attention should be paid to medical technologies which make it possible to uncover the most intimate information on the state of an employee's health. Given the rights to respect for privacy and to human dignity, such techniques should be used with care, only if provided for by specific domestic legislation and accompanied by appropriate safeguards. Reference may be made to the Recommendation No. R (94) 11 of the Committee of Ministers to member States on screening as a tool of preventive medicine. In addition, employers, both in the public and private sectors, should be made aware of the provisions of Recommendation No. R (87) 25 of the Committee of Ministers to member States concerning a common European public health policy to fight the acquired immuno-deficiency syndrome (AIDS). In that recommendation, the Committee of Ministers discourages the use of compulsory screening for the entire population or for particular groups. It is

felt desirable that employers should follow this approach in the employment sector by not obliging job applicants to undergo AIDS screening against their will.

76. The principles laid down earlier in the recommendation in regard to the processing of personal data must be read in the light of the provisions relating to sensitive data set out in Article 6 of Convention 108. These principles seek to adapt this article to the requirements of the employment sector for which there should be no exception other than the one referred to in domestic law, for instance when processing is necessary for the purpose of pension systems or sickness insurance schemes negotiated by employers and trade unions, on condition that appropriate safeguards are provided. The additional safeguards should mainly ensure the security and lawful processing of the data. As regards to cases not covered by this exception, the prohibition on the processing of sensitive data remains the rule; derogation from this rule is only possible if domestic law lays down appropriate safeguards. Moreover, the attention of employers should be drawn to the strict prohibition of collecting sensitive data that are irrelevant to the nature of employment and could lead to discrimination towards specific employees; for instance, rejecting candidates for employment due to their religious or political beliefs or isolating or dismissing an employee owing to his or her sexual preferences.

77. On the other hand, certain types of sensitive data could be processed lawfully when the very nature of the employment requires sensitive data to be obtained: for example, political organisations which seek to influence public opinion may require information on the political views of candidates for posts with such organisations; and religious institutions may require candidates for employment with them to state their religious convictions at the time of recruitment. However this processing is only lawful when specific and additional appropriate safeguards are provided for by domestic law.

78. Principle 9.2 sets out the situations where health data are likely to be processed in the employment context. They relate to both physical and mental health. Principles 9.2 and following are structured in such a way as to limit the processing of health data while emphasising the need for security. As regards to the collection, Principle 9.2 places restrictions on the sort of health data which may be collected. It will be noted that health data concerning prospective employees as well as employees are covered.

79. Principle 9.2.*a* deals with the suitability of the employee to exercise his or her duties. According to this principle, health data can only be obtained if needed to determine whether the employee is fit for a particular position, for example a scientist participating in an expedition. The need to process health-related data has to be evaluated against the purpose for each specific case. The reference to “the requirements of preventive medicine” in Principle 9.2.*b*, covers periodic check-ups, for example to ensure that employees who are exposed to toxic substances in their work environment do not develop any disease. Principle 9.2.*c* allows health data to be collected in order to enable an employee to work under appropriate conditions in line with his/her illness or disability. Processing of health data carried out on the grounds of safeguarding the vital interest of the data subject or other employees, as stated in Principle 9.2.*d*, is usually related to an emergency context, which will be evaluated on a case-by-case basis. Principle 9.2.*e* allows health data to be collected so as to allow “social benefits” to be granted to an employee. For example, an employee injured in the workplace who makes a claim under a company insurance scheme may need to be medically examined to determine the nature and extent of the disability. Moreover, industrial injuries schemes or employees’ compensation schemes administered by the State may require data to be collected on the state of the health of an employee with a view to settling a claim made by the employee or with a view to assessing the likelihood of future claims against the State fund.

80. The nature of the employment will of course influence the sort of questions which may be asked of an employee or applicant, and thus the amount of data which can be collected. It will also influence the nature of the physical examination. For example, an applicant for a job in a nuclear power plant may, in addition to a rigorous medical test, be required to supply information regarding the incidence of cancer or other diseases in his or her family history. Applicants for jobs in the liberal professions would not be expected to do so.

81. Principle 9.3 recalls that respect for rights and fundamental freedoms should be safeguarded during the collection of data. In this regard, it prohibits the processing of genetic data of employees by the employer, as it can lead to discrimination when it comes to any aspect of employment. The processing of genetic data can only be allowed under very exceptional circumstances, regulated by provisions of domestic law. According to Recommendation No. R (97) 5, such processing can only be permitted for health reasons and in particular to avoid any serious prejudice to the health of the data subject or third parties. Processing of genetic information may be acquired for example through a genetic monitoring programme that monitors the biological effects of toxic substances in the workplace, where the monitoring is required by law or, under carefully defined conditions, where the programme is voluntary.

82. Reference should be made to Recommendation No. R (92) 3 of the Committee of Ministers to member States on genetic testing and screening for health care purposes, and in particular to Principle 6 of

the recommendation which provides that "(…) admission to, or the continued exercise of certain activities, especially employment, should not be made dependent on the undergoing of genetics tests or screening". Principle 6 further sets out that "exceptions to this principle must be justified by reasons of direct protection of the person concerned or of a third party and be directly related to the specific conditions of the activity".

83. Principle 9.4 stipulates that an employer can only obtain the data from the employee concerned and is not allowed to collect health data directly from other sources, for example by contacting a former employer. The individual should be the primary source of information for the purposes of supplying health information – primarily through his or her physical examination and answers to the questions put to him or her to determine their suitability for employment, on condition that such processing is lawful.

84. Principle 9.5 relates to situations where personnel bound by "medical confidentiality" may have access to confidential health data for medical reasons. These situations should only be related to the suitability of the employee to exercise his or her duties or to when the processing of health data by the employer is necessary to impose measures to protect the employee's health or to prevent risks for others. It should be noted that, in Principles 9.5 and 9.6, the drafters of the recommendation made a deliberate distinction between health data in general and health data covered by medical confidentiality. It goes without saying that the latter require particular protection.

85. Subject to the rules on the collection of personal data governed by medical confidentiality, referred to in Principles 9.5 and 9.6, and unlike the other categories of sensitive data referred to in Principle 9.1, the processing of data relating to the health of employees or prospective employees is not subject to a requirement of "particular cases". It is accepted that the processing of such data is a generalised and necessary practice in the employment sector. Domestic law will determine the sort of data which are covered by medical confidentiality.

86. Where a company or organisation employs its own medical staff to conduct medical examinations on employees or job applicants, it is essential that they maintain confidentiality at all levels and even before the employer. Employers should not receive medical information, but only conclusions relevant to the employment decision. The categories of persons, other than doctors, who are bound by rules on medical confidentiality, should be determined in accordance with national law and practice. Principle 9.5 places severe limitations on the communication of medical data *sensu stricto* to administrative personnel, it being understood that general indications on the state of health of an employee or prospective employee can be given (X has passed his medical examination; the results of the medical examination reveal that Y is no longer sufficiently fit to continue employment, etc.). Where it is the case that health data have to be communicated to the personnel administration, the data so communicated may only be subsequently stored within the personnel administration in strict compliance with Principles 5 and 6 of this recommendation.

87. The confidentiality of health data is threatened when they are added to an employment record containing various other categories of data. Physical separation also allows for increased data security. Consideration should be given to the use of passwords for selective access to the data stored so as to ensure that only members of the medical service can access the data. Other technical means can be used to prevent unauthorised access.

88. It is recognised that the processing of health data may require the co-operation of persons outside the medical service, who are not subject to the same codes of ethics or requirements of medical confidentiality – for example information technology (IT) staff. It is of the utmost importance that their attention is drawn to the sensitivity of the information being processed and to the need to respect its confidential nature.

89. As regards to the processing of any health data relating to third parties (see Principle 9.7), reference could be made to family members of the employee in order to grant them specific benefits.

10. Transparency of processing

90. Principle 10 proposes a number of ways in which employees can be informed of both their rights and the data processing activities of the employer. A particularly clear and complete description must be provided of the type of personal data which can be collected by means of information systems and technologies which enable them to be monitored by the employer, and of their possible use. A general policy should explain, moreover, how covert surveillance could happen.

91. A similar description should be provided of the use of biometric and of Radio Frequency Identification (RFID) technology, the possible use of personal identification codes and also the role of IT staff (such as system administrators) in relation to data processing.

92. The information should also refer to the rights of the employee in regard to his or her data, as provided for in Principle 11 of this recommendation, as well as the ways and means of exercising those rights. The information referred to in Principle 10.1 should be provided and updated in due time and, in any event, before the employee carries out the activity or action concerned, and should also be made readily available through the information systems normally used by the employee.

93. It should be noted here that the term “recipient”, included in the type of information to be provided to employees, should be understood as a natural or legal person, public authority, service, agency or any other body to whom data are disclosed or made available.

94. In accordance with domestic law or practice and, where appropriate, in accordance with relevant collective agreements, employers should, in advance, fully inform or consult their employees or representatives about the introduction, adaptation and operation of information systems and technologies for the collection and use of personal data necessary for requirements relating to production or safety, or to work organisation.

11. Right of access, rectification and to object

95. Employees should be entitled to know about the personal data processed relating to them. Principle 11.1 advocates that each employee should, on request, be able to access all personal data held by the employer which concern him or her. The employee should also be granted the right to know any available information as to their source, the parties to which the data have been, or could be, communicated and/or the reasoning behind any automated process concerning him or her. To that end, the employer should introduce general procedures to ensure that there is an adequate and prompt response where the right of access, deletion and rectification are exercised, in particular in large-scale entities or entities spread out across the country.

96. The term “controller”, stated in Principle 11.1, refers to the person or body having the decision-making power concerning the processing, whether this power derives from a legal designation or from factual circumstances. In some cases, there may be multiple controllers or co-controllers (jointly responsible for processing and possibly responsible for different aspects of that processing). For the principles set out in this recommendation, the controller is usually the employer. The “processor”, referred to in Principle 20.1, is a separate entity acting on behalf of the controller carrying out the processing in the manner that was requested by the controller and for the needs of the controller. An employee of a controller is not a processor, but a data subject, in respect of the processing of his or her personal data.

97. Under Principle 11.2 each employee should further have the right to request rectification, blockage or erasure of his/her data when they are held contrary to the law or to the principles set out in this recommendation, in particular when they are incorrect. The right to object may be limited by virtue of a law when, for example, the data should be processed pursuant to tax or social security or industrial safety legislation. The right to object may not be applicable when the processing is necessary for employment purposes, such as the execution of a contract of employment.

98. The right of access should also be guaranteed in respect of personal assessment data, referred to in Principle 11.3, including when they relate to assessments of the productivity or capability of the employee (see paragraph 5.5), when the assessment process has been completed at the latest, without prejudice to the right of defence of employers or third parties involved. Principle 11.3 seeks to find a balance between the right of access of the employee, which also extends to evaluation data, with the legitimate need of the employer to express evaluation of the employee. On the other hand, the employee should have a means of appeal for challenging the assessment and defend him/herself against any negative assessment, preferably before the evaluation is finalised. Any deferment for defence purposes shall only be temporary.

99. Principle 11.4 recognises the right of an employee to have his or her views taken into account when subject to a decision solely based on an automated processing of data which has an adverse effect on him or her (for example, a disciplinary measure, a dismissal, a denial of promotion). This could be the case for example when an employee is dismissed for not performing his or her duties on the basis of monitoring carried out via video surveillance, when this monitoring is lawful, and the decision of dismissal is based solely on the images recorded. In addition, the fact that a decision is based on automatic processing cannot deprive the employee of the right to know the reasons on which the decision is based.

100. Principle 11.5 is connected to the previous one, since the implementation of the requirements of Principle 11.4 necessitates the employee being informed of the reasoning on which the automated decision is based, and for this purpose he or she should be entitled to consult and examine the relevant reasoning.

101. Principle 11.6 defines the authorised exceptions to Principles 10, 11.1, 11.2, 11.4 and 11.5. The rights of the employee are not unrestricted and they have to be reconciled with other rights and legitimate interests. They can, in accordance with Convention 108, be limited only where laid down by law and where this constitutes a necessary measure in a democratic society in the interest of legitimate grounds exhaustively listed by Convention 108. For instance, the right to be informed about the reasoning on which processing is based can be limited to protect the rights of others, such as legally protected secrets (e.g. trade secrets). As regards the right to object, the employer may have a compelling legitimate ground for the processing, which overrides the interests or rights and freedoms of the employee. The legitimate interest will, of course, have to be demonstrated on a case-by-case basis in order to pursue such processing. Moreover, there may be practical limitations to an exercise of the right of access. For example, a particular data file may contain data on several employees. In such a case, the employer may extrapolate the personal data referring to the employee concerned and when it is not possible to separate the data of the employee concerned from that of his or colleagues, the employer may be obliged to seek the colleagues' consent before being granted access to the specific data file.

102. The limitation on the exercise of rights expressed in Principle 11.7 applies to, for example, the opening of an investigation by an employer into cases of theft of goods from a factory or from employees. It should be noted that, if the exercise of the right of access has been suspended – and this may only be carried out to an extent necessary for the needs of the investigation – such suspension may not last beyond the end of the inquiry.

103. The person designated by the employee in accordance with the provisions of Principle 11.8 may be a colleague, a lawyer or his or her representative. What is essential is that the employee himself or herself must appoint such a person. Principle 11.8 accepts that domestic law may restrict, or even prohibit, the assistance offered to the employee.

104. Domestic law will further determine the nature of the remedy envisaged in Principle 11.9. Such remedies presuppose the intervention of an independent authority, whether a court or independent body as understood by the Additional Protocol to Convention 108, i.e. one having the power to investigate and to order appropriate sanctions.

12. Security of data

105. Principle 12.1 deals with the technical and organisational steps which should be taken to ensure data security. One way of implementing this recommendation is by legal means; other means might be considered involving the establishment of internal security policies and procedures. Practical precautions also have to be taken by the controller to avoid any accidental or malicious processing incidents. The level of security must be appropriate to the likelihood and severity of risks of the data processing and the nature of personal data, as well as the nature, scope, context and purpose of the processing.

106. Adequate technical and organisational measures, as stated in Principle 12.1, should be adapted according to each situation and should ensure effective data protection. For example:

a. updated processing inventories;
b. privacy impact assessments for high-risk processing operations;
c. the appointment of a data protection officer or a more precise assignment of responsibility to ensure more structured management of data processing; the introduction of internal audit mechanisms or independent inspection of the state of progress in applying legislation;
d. the identification of internal procedures aimed at highlighting security risks or breaches;
e. training activities and certification at various levels, including management.

Furthermore, it should be borne in mind that the minimisation of data provides preventive benefits from the very beginning of the processing. Also where data breaches occur, the employer should implement appropriate technological protection measures to prevent prejudice to employees' rights and should communicate the data breach, without undue delay, to the employees concerned.

107. Principle 12 concerns not only employers, but also third parties, such as employment agencies and IT companies processing the personal data of employees on behalf of employers ("entities which may process data on their behalf"). Reference shall be made in this regard to the obligations of the "processor". The "processor" is a separate entity acting on behalf of the controller carrying out the processing in the manner that was requested by the controller and for the needs of the controller (see also paragraph 90). The rules on security of processing imply an obligation on the controller and the processor to implement

appropriate technical and organisational measures in order to prevent any unauthorised interference with data processing operations [see Directive 95/46/EC].

108. Principle 12.3 sets out the obligations of the personnel administration, as well as other people engaged in the processing of the data, such as webmasters, who, in the exercise of their duties relating to the normal functioning and the security of networks, have access to a certain amount of personal data though mailboxes, login files, temporary files or cookies. This principle provides that the employer should inform the personnel involved in the processing of data about the security measures they should apply, preferably by means of internal policy rules. Another measure would consist of including a clause of confidentiality in their contract and, as the case may be, in the IT charter of the establishment or in the internal regulations.

13. Preservation of data

109. Principle 13.1 provides that the length of time for which personal data can be retained by an employer should be determined by the employment purposes indicated in Principle 2 of the recommendation. For some employment purposes, the length of time that data are to be kept will be longer than for other purposes. The period of preservation will be determined on a case-by-case basis. For example, payment of a company pension scheme will oblige the employer to retain data long after the employee has retired.

110. Principle 13.2 devotes particular attention to the case of personal data submitted by prospective employees. In principle, such data should be deleted when the candidate's application is rejected. In addition, the documents provided by the applicant should either be returned to the applicant or be deleted from the system (online applications for instance). This said, it may sometimes happen that an employer may wish to retain information on a particular candidate who has, for example, failed to meet the requirements of the job description but who could be considered for another post at a later stage and for which he or she is more suited. It may also be in the interests of the rejected prospective employee to have his or her information kept on the employer's databases. Nevertheless, the employer should do so only with the consent of the prospective employee concerned, after he or she has been duly informed.

111. Principle 13.3 also considers the possibility of data submitted in furtherance of a job application being retained by the employer as a precaution against legal action being taken against him by a failed applicant, as well as for other legitimate purposes. For example, the employer may wish to prove to a court that the job applicant was not rejected on grounds of sex, ethnicity, religion, etc., or that correct recruitment and interview procedures were followed. In such cases data should be stored only for the period necessary for the fulfilment of the said purpose, and deleted when the period during which a legal action could have been introduced has expired. The data submitted should also be stored when necessary for other legitimate purposes. For instance, this might be the case when an employer is legally obliged to provide information about circumstances in their activities that are of importance for the supervision of a law, e.g. legislation on non-discrimination. In such cases, the data should be stored as long as necessary.

112. According to Principle 13.4, when an internal investigation is carried out and does not give rise to any charge or negative measure against the employee concerned, the data should be deleted after a reasonable period. There are no rules as to what would constitute a reasonable period. As stated earlier, the length of preservation will be determined on a case-by-case basis. Special attention should be drawn to the right of access of the employee concerned. If the exercise of this right was suspended for the needs of the investigation, personal data processed for the purposes of the investigation should be communicated to the employee concerned before their deletion.

Part II – Particular forms of processing

14. Use of the Internet and electronic communications in the workplace

113. Employers have the right to encourage efficient management and to protect themselves against liabilities and damages which employees' actions may give rise to. Monitoring and surveillance activities in the interests of the employer should however be lawful, transparent, effective and proportionate, and this reasonable approach would also avert possible negative effects on the quality of their professional relationship.

114. To prevent unjustifiable interferences with individuals' rights to private life and to the protection of personal data with regard to the possible processing of personal data relating to Internet or intranet use, employers could be made to formally communicate the information to the persons concerned, outlined in Principle 16.1, in a document such as an IT charter or privacy policy, which should be signed by employees

and periodically updated. The information in the policy on the use of media and on monitoring should be clear, comprehensive, accurate and easily accessible.

115. Principle 14.1 extends to all aspects of an employee's employment, including his or her use of any computer, smartphone or other digital device, either in the framework of the employer's intranet or extranet, or by their direct or indirect use of the Internet provided by the employer. It applies whether the device used by the employee is provided by the employer or by the employee him/herself.[6] Furthermore, it is often the case that information devices in the workplace are used for purposes other than professional ones. Although this should remain appropriate and fair and should not affect either the network's security or the productivity of the establishment, the employer may determine the conditions and restrictions on the use of the Internet that do not constitute a disproportionate infringement of employees' privacy.

116. Principle 14.2 provides for the processing of personal data relating to Internet or intranet pages viewed by the employees. According to this principle the employer may adopt appropriate measures in order to reduce the risk of improper use of the Internet (browsing of non-relevant sites, file or software uploads or downloads, the use of network services for purposes unrelated to work), even by using filters, thus avoiding subsequent processing of employees' personal data which could also involve sensitive data.

117. The employer could, for example, take the following measures:

a. identify and specify a priori the categories of sites which are definitely not related to work;
b. ensure that, when necessary, during screening/check-ups, only data that is anonymous or that does not allow the immediate identification of users is processed through appropriate data aggregation techniques (for example, analysis of log files relating to web traffic of groups of employees only).

118. Principle 14.3 lays down the conditions of lawfulness of access to employees' professional electronic communications. It should be noted that, for the purposes of the recommendation, "professional communications" shall refer particularly to e-mails sent or received during the performance of the employees' duties, or professional information exchanged via Internet messaging services. Access to professional electronic communications may be necessary in order to obtain confirmation or proof of misconduct or in order to detect infringements of employer's intellectual property. When it is professionally necessary to access such communications, employers should demonstrate the security needs or other lawful reasons for that access (such as when the employer is to be held liable for the actions of its employees, has to detect the presence of viruses or guarantee the security of the information system). Employers should take further necessary measures and consider appropriate procedures in order to access an employee's professional electronic communications. For example, if an employee is absent from work unexpectedly and/or for a prolonged period, in view of the possible need for the employer to access the contents of e-mail messages on account of pressing requirements related to work, the employee in question should be allowed to entrust another employee (trusted party) with checking the contents of his/her e-mail messages and forwarding messages that are considered to be professionally relevant to the employer.

119. In addition to providing compelling legitimate grounds for access to professional electronic communications of employees, employers should furthermore inform employees in advance of the existence of this possibility, preferably by means of an explicit internal policy. A proper policy shall therefore clarify the legitimate expectations of employees or third parties to the confidentiality of their communications.

120. It may on some occasions be difficult to distinguish a professional communication from a personal one. In some countries, the content of electronic communications – together with certain data outside of these communications and attached files – is protected by a guarantee of confidentiality of correspondence and communication, sometimes determined at the constitutional level. At least at the beginning, access should in principle be limited to data about the communication (length, recipient, etc.) rather than the content of the communication itself, if this is sufficient to satisfy the employer's needs.

121. Principle 14.4 upholds that private communications at work should not be monitored, including the content, as well as information on sending and receiving.

122. Principle 14.5 sets out the situations where employees leave the organisation. It is stipulated that employers should deactivate former employees' accounts in such a way as to avoid having access to their communication after their departure. If the employers wish to recover the content of an employee's account, they should take the necessary measures to do so before their departure, and preferably in their presence.

[6] See the guidelines on "Bring Your Own Device" (BYOD) issued by the Information Commissioner's Office (ICO) http://ico.org.uk/for_organisations/data_protection/topic_guides/online/byod

123. Principles 14.1 to 14.5 should be interpreted in the sense that all interference with private communications must be in conformity with Article 8 of the ECHR and the corresponding case law of the Court.

15. Information systems and technologies for the monitoring of employees, including video surveillance

124. Principle 15.1 sets strict conditions in respect of the introduction and use of information systems and technologies for monitoring employees' activity and behaviour. Without prejudicing measures relating to well-founded defence proceedings, the use of information systems and technologies, such as video surveillance in the workplace or geolocation systems, should be limited only to organisational and/or production necessities, or for security purposes or the protection of health. Such systems should only be allowed if legitimate, necessary, proportionate, fair, transparent and regulated. They should not aim at permanently monitoring the quality and quantity of the individual work in the workplace, nor aim at remotely monitoring employees' behaviour or location.

Moreover, with regard to video surveillance systems, employers should adopt preventive measures, such as:

- the shortest possible maximum preservation period, to be defined and allowed for by the system;
- only allowing images to be accessed and viewed by duly authorised staff in the exercise of their duties (for example the person responsible for security in the establishment).

125. Principle 15.2 states that the processing of personal data in connection with the use of information systems and technologies must uphold employees' fundamental rights and freedoms and in particular their right to respect for privacy. This approach is consistent with the position adopted by the Court, which has stated repeatedly that increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data. With regard to video surveillance systems, it is clearly stated within Principle 15.2 that placing cameras at locations such as toilets or cloakrooms ("occurrences that are part of the most personal area of life of employees") is strictly prohibited in any situation.

126. While bearing in mind that video surveillance systems are also covered by information systems and technologies, according to the "Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance" adopted by the European Committee on Legal Co-operation (CDCJ) of the Council of Europe in May 2003, "any video surveillance activity should be undertaken by taking such measures as are necessary in order to ensure that this activity complies with personal data protection principles, in particular by only using video surveillance if, depending on the circumstances, the purpose cannot be attained by measures which interfere less with privacy, provided that the alternative measures would not involve disproportionate cost […] and by preventing the data collected from being indexed, matched or kept unnecessarily. When it proves necessary to keep data, these data must be deleted as soon as they are no longer necessary for the determined and specific purpose sought […]."

127. Principle 15.3 stipulates that, in the event of a lawsuit or counterclaim, employees should be able to found it on the recording made. Nonetheless, the application of this principle should not lead to the storage of the recording made for an unlimited and disproportionate period of time and the data protection principles set forth in Principle 3 should apply accordingly.

16. Equipment revealing employees' location

128. Principle 16.1 refers to the use of equipment which may reveal employees' locations and may track their movements. This could be for instance Radio Frequency Identification technologies (commonly known as "RFID technology"), GPS (Global Positioning System) or portable devices, placed inside objects, clothes or uniforms. The considerations discussed under Principle 15.1 are equally valid for the interpretation of Principle 16.1, limiting the use of such equipment only to organisational necessities, or for security and safety purposes, or for the protection of health, in line with the principles of proportionality and legitimacy and on condition that their introduction will not lead to a continuous monitoring of the employees concerned.

129. The use of such equipment may constitute an infringement of the rights and freedoms of employees and should not lead to continuous monitoring of an employee. Preventive measures must be considered, for instance the possibility to suspend the geolocation outside working hours.

130. Furthermore, as far as the implementation of Principle 16.1 is concerned, the use of these devices should not enable the processing of data with regard to certain offences (speeding, for example), nor enable the geolocation of other people.

131. In this context, a particularly clear and complete description must be provided to employees concerned before the use of the equipment which reveals their location. At the very least, the notification should inform employees of the type of personal data which may be collected by means of the equipment, of their possible use and also the role of any system administrators in relation to data processing. Such notification with regard to the policy on monitoring shall also remain valid for other particular forms of processing referred to in Part II of this recommendation.

17. Internal reporting mechanism

132. Internal mechanisms such as hotlines, specific e-mail addresses or online systems may enable employees to report illegal activities. Recommendation CM/Rec(2014)7 of the Committee of Ministers to member States on the protection of whistleblowers, as well as Opinion 1/2006 of the Article 29 Working Party[7] on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime may provide further guidance on this topic. The term “whistleblower” usually refers to a person who reports or discloses misconduct, alleged dishonest or illegal activity occurring in an organisation, in the context of their work-based relationship, whether it is in the public or private sector.

133. Principle 17 underlines the importance of data security and its specific aims. It states that appropriate security measures should be put in place by employers and personal data should be processed for the purpose of internal reporting mechanisms relating to the report, as well as for the purpose of complying with legal obligations deriving from national law or following a legal action brought on the basis of the internal reporting.

134. Those people subject to internal reporting should be duly informed about the use of their data, in order to exercise their rights referred to in paragraph 11.

135. Even if anonymous reporting is possible, other mechanisms should be preferred in order to protect the rights and interests of all parties involved, confidentiality being the rule under all circumstances.

18. Biometric data

136. Principle 18 deals with the processing of biometric data for employment purposes. In information technology, biometrics usually refers to technologies for measuring and analysing human body characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns and hand measurements, especially for authentication purposes. The application of biometrics raises important human rights issues, given that the integrity of the human body and human dignity are at stake.[8]

137. As outlined in Principle 18.1, the processing of biometric data to identify or authenticate employees should, in principle, only be permitted where it is necessary to protect the legitimate interests of the employer, employees or third parties, provided that such interests do not override the fundamental rights of employees. Legitimate interests may prevail, for instance, when protecting the vital interests of employees, or when it is necessary to control access to particularly sensitive areas in terms of security, such as a nuclear plant or a military base.

138. Although the use of biometrics is possible under specific circumstances, employers should use less intrusive means, that is to say methods which uphold individuals’ fundamental rights and freedoms and in particular their right to respect for privacy and to human dignity.

139. Where the use of biometric data is permitted under Principle 18.1, the access to such data shall be subject to requirements of security and proportionality. Biometric data should not be stored in a centralised database, and preference should be given, where appropriate, to biometric identification or authentication systems based on media available solely to the person concerned, thus enabling employees to keep the data themselves, on a card for example.

19. Psychological tests, analysis and similar procedures

[7] The Article 29 Data Protection Working Party is an advisory body and was set up under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[8] See also Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005), prepared by the Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (T-PD).

140. Psychological tests are used generally to determine, among other things, the ability of an employee to work under stressful conditions and to assess the potential of a prospective employee to handle the job effectively under those conditions.

141. According to Principle 19.1, recourse to psychological tests, analyses and similar procedures should not take place unless they are legitimate and necessary in the employment context and domestic law provides appropriate safeguards. In this regard, decisions based solely on the results of such tests, analysis and similar procedures should be challengeable. Psychological testing should be administered by a professional organisation or a psychologist, subject to codes of ethics or requirements of medical confidentiality. The individual's profile should under no circumstances reveal health-related information.

142. Principle 19.2 further provides that the employee or prospective employee concerned should be informed in advance of the use that will be made of the results of these tests, as well as the content of the results.

20. Other forms of data processing posing specific risks to employees' rights

143. With regard to data processing, cloud computing is one example that presents a specific risk to employees' rights. When public bodies and private enterprises use the services of a cloud provider, data are stored or processed by a cloud provider and/or its subcontractors. In such cases, employees risk losing control over their personal data as well as having insufficient information with regard to how, where and by whom the data is being processed/sub-processed. Similar concerns around employees' data privacy rights may be raised by the use of mobile devices at work. The functioning of such devices, allowing for example device-activity monitoring, tracking and remote lock, necessarily involves access to personal data contained in these devices and the processing of this data by the employer.

144. Principle 20.1 draws inspiration from Principle 12 of the recommendation regarding the security of data. Before carrying out data processing, the employer and, where applicable, the processor will have to perform an analysis of its potential impact on the rights and fundamental freedoms of the data subjects. This analysis will also have to take into account the principle of proportionality, on the basis of the comprehensive overview of the processing (that is the entire documentation and description of the processing, indicating what personal data will be processed and for what purpose, how it will be collected, how it will be used, internal flows, disclosures, security measures, etc.). The assistance of IT systems developers, including security professionals, or designers, together with users and legal experts, in analysing the risks would be an advantage and could reduce the administrative burdens linked to this exercise.

145. In order to minimise the risks, employers could for example train staff in charge of processing personal data, set up appropriate notification procedures (for instance to indicate when data has to be deleted from the system), establish specific contractual provisions where the processing is delegated, as well as set up internal procedures to enable the verification and demonstration of compliance. One possible measure that could be taken by the employer to facilitate such a verification and demonstration of compliance would be the designation of a "data protection officer" entrusted with the means necessary to fulfil his or her mission independently. Such a data protection officer, whose designation should be notified to the supervisory authority, could be internal or external to the controller.

146. Principle 20.2 further provides for the consultation of employees' representatives before the introduction of high-risk processing operations, unless domestic law provides other safeguards.

21. Additional safeguards

147. Principle 21 was introduced in order to outline the obligations of the employers when using particular forms of processing, especially those that could lead to the monitoring of employees.

148. Regarding the obligation to inform employees before the introduction of information systems and technologies enabling the monitoring of their activities, the employer must indicate in a clear and detailed manner how the tools placed at their disposal will be used and whether monitoring will be carried out, and if so, the indicators and methods which will be used.

149. Information on the policy regarding the use of media and on monitoring shall be clear, comprehensive, accurate and easily accessible.

150. The employer should for example specify, where applicable:

a. the internal rules on data and systems security or on the protection of company or professional secrecy, provided for all employees, as well as the role of the systems administrator and any relocation of servers to other countries;
b. any personal use of electronic communication tools which is permitted and invoiced to the party concerned or which is strictly forbidden (for example, the downloading or possession of software or files that are wholly unrelated to work activity), providing an indication also of the possible consequences, preferably graduated according to the seriousness of the offence (also taking into account the possibility of involuntary visits to websites due to unexpected actions by search engines, advertisements or typing errors);
c. any inspection that the employer reserves the right to perform, providing an indication of the legitimate reasons for it and the methods used;
d. the log files, if any are kept, in the form of back-up copies as well, and the people who have access to them.

151. Employees or their representatives should be informed and consulted before the introduction or adaptation of any surveillance system. Where the consultation procedure reveals a possibility of infringing an employee's right to respect for privacy and human dignity, his or her agreement should be sought.

152. In situations where there are no employees' representatives, some other specific entities should be involved in order to ensure that such particular forms of processing are carried out with the appropriate safeguards for the employees.

153. Ensuring that a risk analysis be carried out when the introduction of new processing is being considered could also constitute a welcome additional safeguard.

September 2017
This Factsheet does not bind the Court and is not exhaustive

Surveillance at workplace

Article 8 (right to respect for private and family life, home and correspondence) of the European Convention on Human Rights provides that:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

In order to determine whether the interference by the authorities with the applicants' private life or correspondence was necessary in a democratic society and a fair balance was struck between the different interests involved, the European Court of Human Rights examines whether the interference was in accordance with the law, pursued a legitimate aim or aims and was proportionate to the aim(s) pursued.

Monitoring of telephone and internet use

Halford v. the United Kingdom

25 June 1997 (judgment)

The applicant, who was the highest-ranking female police officer in the United Kingdom, brought discrimination proceedings after being denied promotion to the rank of Deputy Chief Constable over a period of seven years. Before the European Court of Human Rights she alleged in particular that her office and home telephone calls had been intercepted with a view to obtaining information to use against her in the course of the proceedings.

The European Court of Human Rights held that there had been a **violation of Article 8** of the European Convention on Human Rights as regards the interception of calls made on the applicant's office telephones. It first found that the conversations held by the applicant on her office telephones fell within the scope of the notions of "private life" and "correspondence" and that Article 8 of the Convention was therefore applicable to this part of the complaint. The Court further noted that there was a reasonable likelihood that calls made by the applicant from her office were intercepted by the police with the primary aim of gathering material to assist in the defence of the sex-discrimination proceedings brought against them. This interception constituted an interference by a public authority with the exercise of the applicant's right to respect for her private life and correspondence. Lastly, the Court observed that the Interception of Communications Act 1985 did not apply to internal communications systems operated by public authorities and that there was no other provision in domestic law to regulate interceptions of telephone calls made on such systems. It could not, therefore, be said that the interference was "in accordance with the law", since the domestic law had not provided adequate protection to the applicant against interferences by the police with her right to respect for her private life and correspondence. In this case the Court also

held that there been a **violation of Article 13** (right to an effective remedy) of the Convention, finding that the applicant had bee unable to seek relief at national level in relation to her complaint concerning her office telephones On the other hand, the Court held that there had been **no violation of Article 8** and **no violation of Article 13** of the Convention as regards the calls made from the applicant's home, since it did in particular not find it established that there had been interference regarding those communications.

Copland v. the United Kingdom

3 April 2007 (judgment)

The applicant was employed by Carmarthenshire College, a statutory body administered by the State. In 1995 she became the personal assistant to the College Principal and was required to work closely with the newly-appointed Deputy Principal. Before the Court, she complained that, during her employment at the College, her telephone, e-mail and internet usage had been monitored at the Deputy Principal's instigation.

The Court held that there had been a **violation of Article 8** of the Convention. It recalled in particular that, according to its case-law, telephone calls from business premises are *prima facie* covered by the notions of "private life" and "correspondence". It followed logically that e-mails sent from work should be similarly protected, as should information derived from the monitoring of personal internet usage. Concerning the applicant, she had however been given no warning that her calls would be liable to monitoring and therefore had a reasonable expectation as to the privacy of calls made from her work telephone. The same expectation ought to apply to her e-mail and internet usage. The Court also noted that the mere fact that the data may have been legitimately obtained by the college, in the form of telephone bills, was no bar to finding an interference. Nor was it relevant that it had not been disclosed to third parties or used against the applicant in disciplinary or other proceedings. The Court therefore found that the collection and storage of personal information relating to the applicant's use of the telephone, e-mail and internet, without her knowledge, had amounted to an interference with her right to respect for her private life and correspondence. In the present case, while leaving open the question whether the monitoring of an employee's use of a telephone, e-mail or internet at the place of work might be considered "necessary in a democratic society" in certain situations in pursuit of a legitimate aim, the Court concluded that, in the absence of any domestic law regulating monitoring at the material time, the interference was not "in accordance with the law". Lastly, having regard to its decision on Article 8 of the Convention, the Court did **not** consider it **necessary** in this case **to examine** the applicant's complaint also **under Article 13** (right to an effective remedy) of the Convention.

Bărbulescu v. Romania

5 September 2017 (Grand Chamber – judgment)

This case concerned the decision of a private company to dismiss an employee – the applicant – after monitoring his electronic communications and accessing their contents. The applicant complained that his employer's decision was based on a breach of his privacy and that the domestic courts had failed to protect his right to respect for his private life and correspondence.

The Grand Chamber held, by eleven votes to six, that there had been a **violation of Article 8** of the Convention, finding that the Romanian authorities had not adequately protected the applicant's right to respect for his private life and correspondence. They had consequently failed to strike a fair balance between the interests at stake. In particular, the national courts had failed to determine whether the applicant had received prior notice from his employer of the possibility that his communications might be monitored; nor had they had regard either to the fact that he had not been informed of the nature or the extent of the monitoring, or the degree of intrusion into his private life and correspondence. In addition, the national courts had failed to determine, firstly, the specific reasons justifying the introduction of the monitoring measures; secondly,

whether the employer could have used measures entailing less intrusion into the applicant's private life and correspondence; and thirdly, whether the communications might have been accessed without his knowledge.

Opening of personal files stored on a professional computer

Pending application

Libert v. France (no. 588/13)

Application communicated to the French Government on 30 March 2015

The applicant in this case complains in particular of a violation of his right to respect for his private life arising from the fact that his employer (The French national rail company, SNCF) opened files on his professional computer's hard drive named « D:/personal data » without him being present. He was later struck off because of the contents of the files in question.

The Court gave notice of the application to the French Government and put questions to the parties under Article 8 (right to respect for private life) of the Convention.

Video surveillance

Köpke v. Germany

5 October 2010 (decision on the admissibility)

The applicant, a supermarket cashier, was dismissed without notice for theft, following a covert video surveillance operation carried out by her employer with the help of a private detective agency. She unsuccessfully challenged her dismissal before the labour courts. Her constitutional complaint was likewise dismissed.

The Court declared **inadmissible**, as being manifestly ill-founded, the applicant's complaint under Article 8 of the Convention, finding that the domestic authorities had struck a fair balance between the employee's right to respect for her private life, her employer's interest in the protection of its property rights and the public interest in the proper administration of justice. The Court noted in particular that the measure complained of had been limited in time (two weeks) and had only covered the area surrounding the cash desk and accessible to the public. The visual data obtained had been processed by a limited number of persons working for the detective agency and by staff members of the employer. They had been used only in connection with the termination of her employment and the proceedings before the labour courts. It therefore concluded that the interference with the applicant's private life had been restricted to what had been necessary to achieve the aims pursued by the video surveillance. The Court observed, however, in this case that the competing interests concerned might well be given a different weight in the future, having regard to the extent to which intrusions into private life were made possible by new, more and more sophisticated technologies.

Pending application

Antović and Mirković v. Montenegro (no. 70838/13)

Application communicated to the Montenegrin Government on 3 December 2014

This case concerns the use of video surveillance in university classrooms, which the applicants – two university professors – claim violates domestic data protection law.

The Court gave notice of the application to the Montenegrin Government and put questions to the parties under Articles 8 (right to respect for private life) and 35 (admissibility criteria) of the Convention.

Further reading

See in particular:

- **"Personal data protection"**, factsheet prepared by the Court's Press Unit
- **Handbook on European Data Protection Law**, European Union Agency for Fundamental Rights / Council of Europe, 2014
- Council of Europe **web page** on data protection

Media Contact:
Tel.: +33 (0)3 90 21 42 08

ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN

WP 249

Opinion 2/2017 on data processing at work

Adopted on 8 June 2017

Contents

1 Executive summary

This Opinion complements the previous Article 29 Working Party ("WP29") publications *Opinion 8/2001 on the processing of personal data in the employment context* (WP48)[1], and the 2002 *Working Document on the surveillance of electronic communications in the workplace* (WP55)[2]. Since the publication of these documents, a number of new technologies have been adopted that enable more systematic processing of employees' personal data at work, creating significant challenges to privacy and data protection.

This Opinion makes a new assessment of the balance between legitimate interests of employers and the reasonable privacy expectations of employees by outlining the risks posed by new technologies and undertaking a proportionality assessment of a number of scenarios in which they could be deployed.

Whilst primarily concerned with the Data Protection Directive, the Opinion looks toward the additional obligations placed on employers by the General Data Protection Regulation. It also restates the position and conclusions of Opinion 8/2001 and the WP55 Working Document, namely that when processing employees' personal data:

- employers should always bear in mind the fundamental data protection principles, irrespective of the technology used;
- the contents of electronic communications made from business premises enjoy the same fundamental rights protections as analogue communications;
- consent is highly unlikely to be a legal basis for data processing at work, unless employees can refuse without adverse consequence;
- performance of a contract and legitimate interests can sometimes be invoked, provided the processing is strictly necessary for a legitimate purpose and complies with the principles of proportionality and subsidiarity;
- employees should receive effective information about the monitoring that takes place; and
- any international transfer of employee data should take place only where an adequate level of protection is ensured.

2. Introduction

The rapid adoption of new information technologies in the workplace, in terms of infrastructure, applications and smart devices, allows for new types of systematic and potentially invasive data processing at work. For example:

- technologies enabling data processing at work can now be implemented at a fraction of the costs of several years ago whilst the capacity for the processing of personal data by these technologies has increased exponentially;

[1] WP29, *Opinion 08/2001 on the processing of personal data in the employment context*, WP 48, 13 September 2001, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp48_en.pdf

[2] WP29, *Working document on the surveillance of electronic communications in the workplace*, WP 55, 29 May 2002, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp55_en.pdf

- new forms of processing, such as those concerning personal data on the use of online services and/or location data from a smart device, are much less visible to employees than other more traditional types such as overt CCTV cameras. This raises questions about the extent to which employees are aware of these technologies, since employers might unlawfully implement these processing without prior notice to the employees; and
- the boundaries between home and work have become increasingly blurred. For example, when employees work remotely (e.g. from home), or whilst they are travelling for business, monitoring of activities outside of the physical working environment can take place and can potentially include monitoring of the individual in a private context.

Therefore, whilst the use of such technologies can be helpful in detecting or preventing the loss of intellectual and material company property, improving the productivity of employees and protecting the personal data for which the data controller is responsible, they also create significant privacy and data protection challenges. As a result, a new assessment is required concerning the balance between the legitimate interest of the employer to protect its business and the reasonable expectation of privacy of the data subjects: the employees.

Whilst this Opinion will focus on new information technologies by assessing nine different scenarios in which they can feature, it will also briefly reflect on more traditional methods of data processing at work where the risks are amplified as a result of technological change.

Where the word "employee" is used in this Opinion, WP29 does not intend to restrict the scope of this term merely to persons with an employment contract recognized as such under applicable labour laws. Over the past decades, new business models served by different types of labour relationships, and in particular employment on a freelance basis, have become more commonplace. This Opinion is intended to cover all situations where there is an employment relationship, regardless of whether this relationship is based on an employment contract.

It is important to state that employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Unless in exceptional situations, employers will have to rely on another legal ground than consent—such as the necessity to process the data for their legitimate interest. However, a legitimate interest in itself is not sufficient to override the rights and freedoms of employees.

Regardless of the legal basis for such processing, a proportionality test should be undertaken prior to its commencement to consider whether the processing is necessary to achieve a legitimate purpose, as well as the measures that have to be taken to ensure that infringements of the rights to private life and secrecy of communications are limited to a minimum. This can form part of a Data Protection Impact Assessment (DPIA).

3. The legal framework

Whilst the analysis below is primarily conducted in relation to the current legal framework under Directive 95/46/EC (the Data Protection Directive or "DPD")[3], this Opinion will also

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281, 23/11/1995, p.31-50*, url: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

look toward the obligations under Regulation 2016/679 (the General Data Protection Regulation or "GDPR")[4], which has already entered into force and which will become applicable on 25 May 2018.

With regard to the proposed ePrivacy Regulation[5], the Working Party calls on European legislators to create a specific exception for interference with devices issued to employees[6]. The Proposed Regulation does not contain a suitable exception to the general interference prohibition, and employers cannot usually provide valid consent for the processing of personal data of their employees.

3.1 Directive 95/46/EC—Data Protection Directive ("DPD")

In Opinion 08/2001, WP29 previously outlined that employers take into account the fundamental data protection principles of the DPD when processing personal data in the employment context. The development of new technologies and new methods of processing in this context have not altered this situation—in fact, it can be said that such developments have made it *more* important for employers to do so. In this context, employers should:

- ensure that data is processed for specified and legitimate purposes that are proportionate and necessary;
- take into account the principle of purpose limitation, while making sure that the data are adequate, relevant and not excessive for the legitimate purpose;
- apply the principles of proportionality and subsidiarity regardless of the applicable legal ground;
- be transparent with employees about the use and purposes of monitoring technologies;
- enable the exercise of data subject rights, including the rights of access and, as appropriate, the rectification, erasure or blocking of personal data;
- keep the data accurate, and not retain them any longer than necessary; and
- take all necessary measures to protect the data against unauthorised access and ensure that staff are sufficiently aware of data protection obligations.

Without repeating the earlier advice given, WP29 wishes to highlight three principles, namely: legal grounds, transparency, and automated decisions.

3.1.1 *LEGAL GROUNDS (ARTICLE 7)*

When processing personal data in the employment context, at least one of the criteria set out in Art. 7 has to be satisfied. If the types of personal data processed involve the special categories (as elaborated in Art. 8), the processing is prohibited unless an exception applies[7,8].

---

[4] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119, 4.5.2016, p. 1-88*, url: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[5] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[6] See WP29, *Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation*, WP 247, 04 April 2017, page 29; url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

[7] As stated in part 8 of Opinion 08/2001; for example, Art. 8(2)(b) provides an exception for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorised by national law providing for adequate safeguards.

Even if the employer can rely on one of those exceptions, a legal ground from Art. 7 is still required for the processing to be legitimate.

In summary, employers must therefore take note of the following:

- for the majority of such data processing at work**, the legal basis cannot and should not be the consent of the employees** (Art 7(a)) due to the nature of the relationship between employer and employee;
- processing may be necessary for **the performance of a contract** (Art 7(b)) in cases where the employer has to process personal data of the employee to meet any such obligations;
- it is quite common that **employment law may impose legal obligations** (Art. 7(c)) **that necessitate the processing of personal data**; in such cases the employee must be clearly and fully informed of such processing (unless an exception applies);
- should an employer seek to rely on **legitimate interest** (Art. 7(f)) the purpose of the processing must be legitimate; the chosen method or specific technology must be necessary, proportionate and implemented in the least intrusive manner possible along with the ability to enable the employer to demonstrate that **appropriate measures have been put in place** to ensure a balance with the fundamental rights and freedoms of employees[9];
- the processing operations must also comply with the **transparency requirements** (Art. 10 and 11), and employees should be clearly and fully informed of the processing of their personal data[10], including the existence of any monitoring; and
- **appropriate technical and organisational measures** should be adopted to ensure security of the processing (Art. 17).

The most relevant criteria under Art. 7 are detailed below.

- **Consent (Article 7(a))**

Consent, according to the DPD, is defined as any freely-given, specific and informed indication of a data subject's wishes by which the he or she signifies his or her agreement to personal data relating to them being processed. For consent to be valid, it must also be revocable.

WP29 has previously outlined in Opinion 8/2001 that where an employer has to process personal data of his/her employees it is misleading to start with the supposition that the processing can be legitimised through the employees' consent. In cases where an employer says they require consent and there is a real or potential relevant prejudice that arises from the employee not consenting (which can be highly probable in the employment context, especially when it concerns the employer tracking the behaviour of the employee over time), then the consent is not valid since it is not and cannot be freely given. Thus, for the majority

[8] It should be noted that in some countries, there are special measures in place that employers must abide by to protect employees' private lives. Portugal is one example of countries where such special measures exist and similar measures may apply in some other Member States too. The conclusions in section 5.6 as well as the examples presented in sections 5.1 and 5.7.1 of this Opinion are therefore not valid in Portugal for these reasons.
[9] WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, adopted 9 April 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf.
[10] Pursuant to Art. 11(2) of the DPD, the controller is exempted from the obligation to provide information to the data subject in cases where the recording or collection of data is expressly laid down by law.

of the cases of employees' data processing, the legal basis of that processing cannot and should not be the consent of the employees, so a different legal basis is required.

Moreover, even in cases where consent could be said to constitute a valid legal basis of such a processing (i.e. if it can be undoubtedly concluded that the consent is freely given), it needs to be a specific and informed indication of the employee's wishes. Default settings on devices and/or the installation of software that facilitate the electronic personal data processing cannot qualify as consent given from employees, since consent requires an active expression of will. A lack of action (i.e, not changing the default settings) may generally not be considered as a specific consent to allow such processing[11].

- **Performance of a contract (Article 7(b))**

Employment relationships are often based on a contract of employment between the employer and the employee. When meeting obligations under this contract, such as paying the employee, the employer is required to process some personal data.

- **Legal obligations (Article 7(c))**

It is quite common that employment law imposes legal obligations on the employer, which necessitate the processing of personal data (e.g. for the purpose of tax calculation and salary administration). Clearly, in such cases, such a law constitutes the legal basis for the data processing..

- **Legitimate interest (Article 7(f))**

If an employer wishes to rely upon the legal ground of Art. 7(f) of the DPD, the purpose of the processing must be legitimate, and the chosen method or specific technology with which the processing is to be undertaken must be necessary for the legitimate interest of the employer. The processing must also be proportionate to the business needs, i.e. the purpose, it is meant to address. Data processing at work should be carried out in the least intrusive manner possible and be targeted to the specific area of risk. Additionally, if relying on Art. 7(f), the employee retains the right to object to the processing on compelling legitimate grounds under Art. 14.

In order to rely on Art. 7(f) as the legal ground for processing it is essential that specific mitigating measures are present to ensure a proper balance between the legitimate interest of the employer and the fundamental rights and freedoms of the employees.[12] Such measures, depending on the form of monitoring, should include limitations on monitoring so as to guarantee that the employee's privacy is not violated. Such limitations could be:

---

[11] See also WP29, *Opinion 15/2011 on the definition of consent,* WP187, 13 July 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf, page 24.

[12] For an example of the balance that needs to be struck, see the case of *Köpke v Germany*, [2010] ECHR 1725, (URL: http://www.bailii.org/eu/cases/ECHR/2010/1725.html), in which an employee was dismissed as a result of a covert video surveillance operation undertaken by the employer and a private detective agency. Whilst in this instance the Court concluded that the domestic authorities had struck a fair balance between the employer's legitimate interest (in the protection of its property rights), the employee's right to respect for private life, and the public interest in the administration of justice, it also observed that the various interests concerned could be given a different weight in future as a result of technological development.

- geographical (e.g. monitoring only in specific places; monitoring sensitive areas such as religious places and for example sanitary zones and break rooms should be prohibited),
- data-oriented (e.g. personal electronic files and communication should not be monitored), and
- time-related (e.g. sampling instead of continuous monitoring).

3.1.2 *TRANSPARENCY (ARTICLES 10 AND 11)*

The transparency requirements of Articles 10 and 11 apply to data processing at work; employees must be informed of the existence of any monitoring, the purposes for which personal data are to be processed and any other information necessary to guarantee fair processing.

With new technologies, the need for transparency becomes more evident since they enable the collection and further processing of possibly huge amounts of personal data in a covert way.

3.1.3 *AUTOMATED DECISIONS (ARTICLE 15)*

Art. 15 of the DPD also grants data subjects the right not to be subject to a decision based solely on automated processing, where that decision produces legal effects or similarly significantly affects them and which is based solely on automated processing of data intended to evaluate certain personal aspects, such as performance at work, unless the decision is necessary for entering into or performance of a contract, authorised by Union or Member State law, or is based on the explicit consent of the data subject.

3.2 Regulation 2016/679—General Data Protection Regulation ("GDPR")

The GDPR includes and enhances the requirements in the DPD. It also introduces new obligations for all data controllers, including employers.

3.2.1 *DATA PROTECTION BY DESIGN*

Art. 25 of the GDPR requires data controllers to implement data protection by design and by default. As an example: where an employer issues devices to employees, the most privacy-friendly solutions should be selected if tracking technologies are involved. Data minimisation must also be taken into account.

3.2.2 *DATA PROTECTION IMPACT ASSESSMENTS*

Art. 35 of the GDPR outlines the requirements for a data controller to carry out a Data Protection Impact Assessment (DPIA) where a type of processing, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing itself, is likely to result in a high risk to the rights and freedoms of natural persons. An example is a case of systematic and extensive evaluation of personal aspects related to natural persons based on automated processing including profiling, and on which decisions are taken that produce legal effects concerning the natural person or similarly significantly affect the natural person.

Where the DPIA indicates that the identified risks cannot be sufficiently addressed by the controller—i.e., that the residual risks remain high—then the controller must consult the supervisory authority prior to the commencement of the processing (Art. 36(1)) as clarified in the WP29 guidelines on DPIAs[13].

3.2.2 "*PROCESSING IN THE CONTEXT OF EMPLOYMENT*"

Art. 88 of the GDPR states that Member States may, by law or collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context. In particular, these rules may be provided for the purposes of:

- recruitment;
- performance of the employment contract (including discharge of obligations laid down by law or collective agreements);
- management, planning and organisation of work;
- equality and diversity in the workplace;
- health and safety at work;
- protection of an employer's or customer's property;
- exercise and enjoyment (on an individual basis) of rights and benefits related to employment; and
- termination of the employment relationship.

In accordance with Art. 88(2), any such rules should include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to:

- the transparency of processing;
- the transfer of personal data within a group of undertakings or group of enterprises engaged in a joint economic activity; and
- monitoring systems at the workplace.

In this Opinion, the Working Party has provided guidelines for the legitimate use of new technology in a number of specific situations, detailing suitable and specific measures to safeguard the human dignity, legitimate interest and fundamental rights of employees.

4. Risks

Modern technologies enable employees to be tracked over time, across workplaces and their homes, through many different devices such as smartphones, desktops, tablets, vehicles and wearables. If there are no limits to the processing, and if it is not transparent, there is a high risk that the legitimate interest of employers in the improvement of efficiency and the protection of company assets turns into unjustifiable and intrusive monitoring.

Technologies that monitor communications can also have a chilling effect on the fundamental rights of employees to organise, set up workers' meetings, and to communicate confidentially

[13] WP29, *Guidelines on data protection impact assessment (DPIA) and determining whether processing is likely to result in "high risk" for the purposes of Regulation 2016/679*, WP 248, 04 April 2017, url: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137, page 18.

(including the right to seek information). Monitoring communications and behaviour will put pressure on employees to conform in order to prevent the detection of what might be perceived as anomalies, in a comparable way to the way in which the intensive use of CCTV has influenced citizens' behaviour in public spaces. Moreover, owing to the capabilities of such technologies, employees may not be aware of what personal data are being processed and for which purposes, whilst it is also possible that they are not even aware of the existence of the monitoring technology itself.

Monitoring IT usage also differs from other, more visible observation and monitoring tools like CCTV in that it can take place in a covert way. In the absence of an easily understandable and readily accessible workplace monitoring policy, employees may not be aware of the existence and consequences of the monitoring that is taking place, and are therefore unable to exercise their rights. A further risk comes from the "over-collection" of data in such systems, e.g. those collecting WiFi location data.

The increase in the amount of data generated in the workplace environment, in combination with new techniques for data analysis and cross-matching, may also create risks of incompatible further processing. Examples of illegitimate further processing include using systems that are legitimately installed to protect properties to then monitor the availability, performance and customer-friendliness of employees. Others include using data collected via a CCTV system to regularly monitor the behaviour and performance of employees, or using data of a geolocation system (such as for example WiFi- or Bluetooth tracking) to constantly check an employee's movements and behaviour.

As a result, such tracking may infringe upon the privacy rights of employees, regardless of whether the monitoring takes place systematically or occasionally. The risk is not limited to the analysis of the content of communications. Thus, the analysis of metadata about a person might allow for an equally privacy-invasive detailed monitoring of an individual's life and behavioural patterns.

The extensive use of monitoring technologies may also limit employees' willingness to (and channels by which they could) inform employers about irregularities or illegal actions of superiors and/or other employees threatening to damage the business (especially client data) or workplace. Anonymity is often necessary for a concerned employee to take action and report such situations. Monitoring that infringes upon the privacy rights of employees may hamper necessary communications to the appropriate officers. In such an instance, the established means for internal whistle-blowers may become ineffective[14].

5. Scenarios

This section addresses a number of data processing at work scenarios in which new technologies and/or developments of existing technologies have, or may have, the potential to result in high risks to the privacy of employees. In all such cases employers should consider whether:

[14] See for example WP29, *Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime*, WP 117, 1 February 2006, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp117_en.pdf.

- the processing activity is necessary, and if so, the legal grounds that apply;
- the proposed processing of personal data is fair to the employees;
- the processing activity is proportionate to the concerns raised; and
- the processing activity is transparent.

5.1 Processing operations during the recruitment process

Use of social media by individuals is widespread and it is relatively common for user profiles to be publicly viewable depending on the settings chosen by the account holder. As a result, employers may believe that inspecting the social profiles of prospective candidates can be justified during their recruitment processes. This may also be the case for other publicly-available information about the potential employee.

However, employers should not assume that merely because an individual's social media profile is publicly available they are then allowed to process those data for their own purposes. A legal ground is required for this processing, such as legitimate interest. In this context the employer should—prior to the inspection of a social media profile—take into account whether the social media profile of the applicant is related to business or private purposes, as this can be an important indication for the legal admissibility of the data inspection. In addition, employers are only allowed to collect and process personal data relating to job applicants to the extent that the collection of those data is necessary and relevant to the performance of the job which is being applied for.

Data collected during the recruitment process should generally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the individual concerned[15]. The individual must also be correctly informed of any such processing before they engage with the recruitment process.

There is no legal ground for an employer to require potential employees to "friend" the potential employer, or in other ways provide access to the contents of their profiles.

Example

During the recruitment of new staff, an employer checks the profiles of the candidates on various social networks and includes information from these networks (and any other information available on the internet) in the screening process.

Only if it is necessary for the job to review information about a candidate on social media, for example in order to be able to assess specific risks regarding candidates for a specific function, and the candidates are correctly informed (for example, in the text of the job advert) the employer may have a legal basis under Article 7(f) to review publicly-available information about candidates.

[15] See also Council of Europe, *Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment*, paragraph 13.2 (1 April 2015, url: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a). In cases where the employer wishes to retain the data with a view to a further job opportunity, the data subject should be informed accordingly and be given the possibility to object to such further processing, in which case it should be deleted (Id.).

5.2 Processing operations resulting from in-employment screening

Through the existence of profiles on social media, and the development of new analytical technologies, employers have (or can obtain) the technical capability of permanently screening employees by collecting information regarding their friends, opinions, beliefs, interests, habits, whereabouts, attitudes and behaviours therefore capturing data, including sensitive data, relating to the employee's private and family life.

In-employment screening of employees' social media profiles should not take place on a generalised basis.

Moreover, employers should refrain from requiring an employee or a job applicant access to information that he or she shares with others through social networking.

Example
An employer monitors the LinkedIn profiles of former employees that are involved during the duration of non-compete clauses. The purpose of this monitoring is to monitor compliance with such clauses. The monitoring is limited to these former employees.

As long as the employer can prove that such monitoring is necessary to protect his legitimate interests, that there are no other, less invasive means available, and that the former employees have been adequately informed about the extent of the regular observation of their public communications, the employer may be able to rely on the legal basis of Article 7(f) of the DPD.

Additionally, employees should not be required to utilise a social media profile that is provided by their employer. Even when this is specifically foreseen in light of their tasks (e.g. spokesperson for an organisation), they must retain the option of a "non-work" non-public profile that they can use instead of the "official" employer-related profile, and this should be specified in the terms and conditions of the employment contract.

5.3 Processing operations resulting from monitoring ICT usage at the workplace

Traditionally, the monitoring of electronic communications in the workplace (eg, phone, internet browsing, email, instant messaging, VOIP, etc.) was considered the main threat to employees' privacy. In its 2001 *Working Document on the surveillance of electronic communications in the workplace*, WP29 made a number of conclusions in relation to the monitoring of email and internet usage. While those conclusions remain valid, there is a need to take into account technological developments that have enabled newer, potentially more intrusive and pervasive ways of monitoring. Such developments include, amongst others:

- Data Loss Prevention (DLP) tools, which monitor outgoing communications for the purpose of detecting potential data breaches;
- Next-Generation Firewalls (NGFWs) and Unified Threat Management (UTM) systems, which can provide a variety of monitoring technologies including deep packet inspection, TLS interception, website filtering, content filtering, on-appliance reporting, user identity information and (as described above) data loss prevention. Such technologies may also be deployed individually, depending on the employer;

- security applications and measures that involve logging employee access to the employer's systems;
- eDiscovery technology, which refers to any process in which electronic data is searched with the aim of its use as evidence;
- tracking of application and device usage via unseen software, either on the desktop or in the cloud;
- the use in the workplace of office applications provided as a cloud service, which in theory allow for very detailed logging of the activities of employees;
- monitoring of personal devices (e.g., PCs, mobile phones, tablets), that employees supply for their work in accordance with a specific use policy, such as Bring-Your-Own-Device (BYOD), as well as Mobile Device Management (MDM) technology which enables the distribution of applications, data and configuration settings, and patches for mobile devices; and
- the use of wearable devices (e.g., health and fitness devices).

It is possible that an employer will implement an "all-in-one" monitoring solution, such as a suite of security packages which enable them to monitor all ICT usage in the workplace as opposed to just email and/or website monitoring as was once the case. The conclusions adopted in WP55 would apply for any system that enables such monitoring to take place.[16]

Example

An employer intends to deploy a TLS inspection appliance to decrypt and inspect secure traffic, with the purpose of detecting anything malicious. The appliance is also able to record and analyse the entirety of an employee's online activity on the organisation's network.

Use of encrypted communications protocols is increasingly being implemented to protect online data flows involving personal data against interception. However, this can also present issues, as the encryption makes it impossible to monitor incoming and outgoing data. TLS inspection equipment decrypts the data stream, analyses the content for security purposes and then re-encrypts the stream afterwards.

In this example, the employer relies upon legitimate interests—the necessity to protect the network, and the personal data of employees and customers held within that network, against unauthorised access or data leakage. However, monitoring every online activity of the employees is a disproportionate response and an interference with the right to secrecy of communications. The employer should first investigate other, less invasive, means to protect the confidentiality of customer data and the security of the network.

To the extent that some interception of TLS traffic can be qualified as strictly necessary, the appliance should be configured in a way to prevent permanent logging of employee activity, for example by blocking suspicious incoming or outgoing traffic and redirecting the user to an information portal where he or she may ask for review of such an automated decision. If some general logging would nonetheless be deemed strictly necessary, the appliance may

[16] See also *Copland v United Kingdom,* (2007) 45 EHRR 37, 25 BHRC 216, 2 ALR Int'l 785, [2007] ECHR 253 (url: http://www.bailii.org/eu/cases/ECHR/2007/253.html), in which the Court stated that emails sent from business premises and information derived from the monitoring of internet use could be a part of an employee's private life and correspondence, and that the collection and storage of that information without the knowledge of the employee would amount to an interference with the employee's rights, although the Court did not rule that such monitoring would never be necessary in a democratic society.

also be configured not to store log data unless the appliance signals the occurrence of an incident, with a minimization of the information collected.

As a good practice, the employer could offer alternative unmonitored access for employees. This could be done by offering free WiFi, or stand-alone devices or terminals (with appropriate safeguards to ensure confidentiality of the communications) where employees can exercise their legitimate right to use work facilities for some private usage[17]. Moreover, employers should consider certain types of traffic whose interception endangers the proper balance between their legitimate interests and employee's privacy—such as the use of private webmail, visits to online banking and health websites—with the aim to appropriately configure the appliance so as not to proceed with interception of communications in circumstances that are not compliant with proportionality. Information on the type of communications that the appliance is monitoring should be specified to the employees.

A policy concerning the purposes for when, and by whom, suspicious log data can be accessed should be developed and made easily and permanently accessible for all employees, in order to also guide them about acceptable and unacceptable use of the network and facilities. This allows employees to adapt their behaviour to prevent being monitored when they legitimately use IT work facilities for private use. As good practice, such a policy should be evaluated, at least annually, to assess whether the chosen monitoring solution delivers the intended results, and whether there are other, less invasive tools or means available to achieve the same purposes.

Irrespective of the technology concerned or the capabilities it possesses, the legal basis of Article 7(f) is only available if the processing meets certain conditions. Firstly, employers utilising these products and applications must consider the proportionality of the measures they are implementing, and whether any additional actions can be taken to mitigate or reduce the scale and impact of the data processing. As an example of good practice, this consideration could be undertaken via a DPIA prior to the introduction of any monitoring technology. Secondly, employers must implement and communicate acceptable use policies alongside privacy policies, outlining the permissible use of the organisation's network and equipment, and strictly detailing the processing taking place.

In some countries the creation of such a policy would legally require approval of a Workers' Council or similar representation of employees. In practice, such policies are often drafted by IT maintenance staff. Since their main focus will mostly be on security, and not on the legitimate expectation of privacy of employees, WP29 recommends that in all cases a representative sample of employees is involved in assessing the necessity of the monitoring, as well as the logic and accessibility of the policy.

[17] See *Halford v. United Kingdom*, [1997] ECHR 32, (url: http://www.bailii.org/eu/cases/ECHR/1997/32.html), in which the Court stated that "telephone calls made from business premises as well as from the home may be covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8 paragraph 1 [of the Convention]"; and *Barbulescu v. Romania*, [2016] ECHR 61, (url: http://www.bailii.org/eu/cases/ECHR/2016/61.html), concerning the use of a professional instant messenger account for personal correspondence, in which the Court stated that monitoring of the account by the employer was limited and proportionate; the dissenting opinion of Judge Pinto de Alberquerque which argued for a careful balance to be struck.

Example

An employer deploys a Data Loss Prevention tool to monitor the outgoing e-mails automatically, for the purpose of preventing unauthorised transmission of proprietary data (e.g. customer's personal data), independently from whether such an action is unintentional or not. Once an e-mail is being considered as the potential source of a data breach, further investigation is performed.

Again, the employer relies upon the necessity for his legitimate interest to protect the personal data of customers as well as his assets against unauthorised access or data leakage. However, such a DLP tool may involve unnecessary processing of personal data —for example, a "false positive" alert might result in unauthorized access of legitimate e-mails that have been sent by employees (which may be, for instance, personal e-mails).

Therefore, the necessity of the DLP tool and its deployment should be fully justified so as to strike the proper balance between his legitimate interests and the fundamental right to the protection of employees' personal data. In order for the legitimate interests of the employer to be relied upon, certain measures should be taken to mitigate the risks. For example, the rules that the system follows to characterize an e-mail as potential data breach should be fully transparent to the users, and in cases that the tool recognises an e-mail that is to be sent as a possible data breach, a warning message should inform the sender of the e-mail prior to the e-mail transmission, so as to give the sender the option to cancel this transmission.

In some cases, the monitoring of employees is possible not so much because of the deployment of specific technologies, but simply because employees are expected to use online applications made available by the employer which process personal data. The use of cloud-based office applications (e.g. document editors, calendars, social networking) is an example of this. It should be ensured that employees can designate certain private spaces to which the employer may not gain access unless under exceptional circumstances. This, for example, is relevant for calendars, which are often also used for private appointments. If the employee sets an appointment to "Private" or notes this in appointment itself, employers (and other employees) should not be allowed to review the contents of the appointment.

The requirement of subsidiarity in this context sometimes means that no monitoring may take place at all. For example, this is the case where the prohibited use of communications services can be prevented by blocking certain websites. If it is possible to block websites, instead of continuously monitoring all communications, blocking should be chosen in order to comply with this requirement of subsidiarity.

More generally, prevention should be given much more weight than detection—the interests of the employer are better served by preventing internet misuse through technical means than by expending resources in detecting misuse.

5.4 Processing operations resulting from monitoring ICT usage outside the workplace

ICT usage outside the workplace has become more common with the growth of homeworking, remote working and "bring your own device" policies. The capabilities of such technologies can pose a risk to the private life of employees, as in many cases the monitoring systems existing in the workplace are effectively extended into the employees' domestic sphere when they use such equipment. .

5.4.1 *MONITORING OF HOME AND REMOTE WORKING*

It has become more common for employers to offer employees the option to work remotely, e.g., from home and/or whilst in transit. Indeed, this is a central factor behind the reduced distinction between the workplace and the home. In general this involves the employer issuing ICT equipment or software to the employees which, once installed in their home/on their own devices, enables them to have the same level of access to the employer's network, systems and resources that they would have if they were in the workplace, depending on the implementation.

Whilst remote working can be a positive development, it also presents an area of additional risk for an employer. For example, employees that have remote access to the employer's infrastructure are not bound by the physical security measures that may be in place at the employer's premises. To put it plainly: without the implementation of appropriate technical measures the risk of unauthorised access increases and may result in the loss or destruction of information, including personal data of employees or customers, which the employer may hold.

In order to mitigate this area of risk employers may think there is a justification for deploying software packages (either on-premise or in the cloud) that have the capabilities of, for example, logging keystrokes and mouse movements, screen capturing (either randomly or at set intervals), logging of applications used (and how long they were used for), and, upon compatible devices, enabling webcams and collecting the footage thereof. Such technologies are widely available including from third parties such as cloud providers.

However, the processing involved in such technologies are disproportionate and the employer is very unlikely to have a legal ground under legitimate interest, e.g. for recording an employee's keystrokes and mouse movements.

The key is addressing the risk posed by home and remote working in a proportionate, non-excessive manner, in whatever way the option is offered and by whatever technology is proposed, particularly if the boundaries between business and private use are fluid.

5.4.2 *BRING YOUR OWN DEVICE (BYOD)*

Due to the rise in popularity, features and capability of consumer electronic devices, employers may face demands from employees to use their own devices in the workplace to carry out their jobs. This is known as "bring your own device" or BYOD.

Implementing BYOD effectively can lead to a number of benefits for employees, including improved employee job satisfaction, overall morale increase, increased job efficiency and increased flexibility. However, by definition, some use of an employee's device will be personal in nature, and this is more likely to be the case at certain times of the day (e.g., evenings and weekends). It is therefore a distinct possibility that employees' use of their own devices will lead to employers processing non-corporate information about those employees, and possibly any family members who also use the devices in question.

In the employment context, BYOD privacy risks are commonly associated with monitoring technologies that collect identifiers such as MAC addresses, or in instances where an employer accesses an employee's device under the justification of performing a security scan, i.e. for malware. In respect of the latter, a number of commercial solutions exist that allow for

the scanning of private devices, however their usage could potentially access all data on that device and therefore they must be carefully managed. For example, those sections of a device which are presumed to be only used for private purposes (e.g. the folder storing photos taken with the device) may in principle not be accessed.

Monitoring the location and traffic of such devices may be considered to serve a legitimate interest to protect the personal data that the employer is responsible for as the data controller; however this may be unlawful where an employee's personal device is concerned, if such monitoring also captures data relating to the employee's private and family life. In order to prevent monitoring of private information appropriate measures must be in place to distinguish between private and business use of the device.

Employers should also implement methods by which their own data on the device is securely transferred between that device and their network. It may be the case that the device is therefore configured to route all traffic through a VPN back into the corporate network, so as to offer a certain level of security; however, if such a measure is used, the employer should also consider that software installed for the purposes of monitoring pose a privacy risk during periods of personal usage by the employee. Devices that offer additional protections such as "sandboxing" data (keeping data contained within a specific app) could be used.

Conversely, the employer must also consider the prohibition of the use of specific work devices for private use if there is no way to prevent private use being monitored—for example if the device offers remote access to personal data for which the employer is the data controller.

5.4.3 *MOBILE DEVICE MANAGEMENT (MDM)*

Mobile device management enables employers to locate devices remotely, deploy specific configurations and/or applications, and delete data on demand. An employer may operate this functionality himself, or use a third party to do so. MDM services also enable employers to record or track the device in real-time even if it is not reported stolen.

A DPIA should be performed prior to the deployment of any such technology where it is new, or new to the data controller. If the outcome of the DPIA is that the MDM technology is necessary in specific circumstances, an assessment should still be made as to whether the resulting data processing complies with the principles of proportionality and subsidiarity. Employers must ensure that the data collected as part of this remote location capability is processed for a specified purpose and does not, and could not, form part of a wider programme enabling ongoing monitoring of employees. Even for specified purposes, the tracking features should be mitigated. Tracking systems can be designed to register the location data without presenting it to the employer—in such circumstances, the location data should become available only in circumstances where the device would be reported or lost.

Employees whose devices are enrolled in MDM services must also be fully informed as to what tracking is taking place, and what consequences this has for them.

5.4.4 *WEARABLE DEVICES*

Employers are increasingly tempted to provide wearable devices to their employees in order to track and monitor their health and activity within and sometimes even outside of the

workplace. However, this data processing involves the processing of health data, and is therefore prohibited based on Article 8 of the DPD.

Given the unequal relationship between employers and employees—i.e., the employee has a financial dependence on the employer—and the sensitive nature of the health data, it is highly unlikely that legally valid explicit consent can be given for the tracking or monitoring of such data as employees are essentially not 'free' to give such consent in the first place. Even if the employer uses a third party to collect the health data, which would only provide aggregated information about general health developments to the employer, the processing would still be unlawful.

Also, as described in *Opinion 5/2014 on Anonymisation Techniques*[18], it is technically very difficult to ensure complete anonymisation of the data. Even in an environment with over a thousand employees, given the availability of other data about the employees the employer would still be able to single out individual employees with particular health indications such as high blood pressure or obesity.

Example:

An organisation offers fitness monitoring devices to its employees as a general gift. The devices count the number of steps employees take, and register their heartbeats and sleeping patterns over time.

The resulting health data should only be accessible to the employee and not the employer. Any data transferred between the employee (as data subject) and the device/service provider (as data controller) is a matter for those parties.

As the health data could also be processed by the commercial party that has manufactured the devices or offers a service to employers, when choosing the device or service the employer should evaluate the privacy policy of the manufacturer and/or service provider, to ensure that it does not result in unlawful processing of health data on employees.

5.5 Processing operations relating to time and attendance

Systems that enable employers to control who can enter their premises, and/or certain areas within their premises, can also allow the tracking of employees' activities. Although such systems have existed for a number of years, new technologies intended to track employees' time and attendance are being more widely deployed, including those that process of biometric data as well as others such as mobile device tracking.

Whilst such systems can form an important component of an employer's audit trail, they also pose the risk of providing an invasive level of knowledge and control regarding the activities of the employee whilst in the workplace.

Example:

An employer maintains a server room in which business-sensitive data, personal data relating to employees and personal data relating to customers is stored in digital form. In order to

[18] WP29, *Opinion 5/2014 on anonymization techniques*, WP 216, 10 April 2014, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

comply with legal obligations to secure the data against unauthorised access, the employer has installed an access control system that records the entrance and exit of employees who have appropriate permission to enter the room. Should any item of equipment go missing, or if any data is subject to unauthorised access, loss or theft, the records maintained by the employer allow them to determine who had access to the room at that time.

Given that the processing is necessary and does not outweigh the right to private life of the employees, it can be in the legitimate interest under Art. 7(f), if the employees have been adequately informed about the processing operation. However, the continuous monitoring of the frequency and exact entrance and exit times of the employees cannot be justified if these data are also used for another purpose, such as employee performance evaluation.

5.6 Processing operations using video monitoring systems

Video monitoring and surveillance continues to present similar issues for employee privacy as before: the capability to continuously capture the behaviour of the worker.[19] The most relevant changes relating to the application of this technology in the employment context are the capability to access the collected data remotely (e.g. via a smartphone) easily; the reduction in the cameras' sizes (along with an increase in their capabilities, e.g. high-definition); and the processing that can be performed by new video analytics.

With the capabilities given by video analytics, it is possible for an employer to monitor the worker's facial expressions by automated means, to identify deviations from predefined movement patterns (e.g. factory context), and more. This would be disproportionate to the rights and freedoms of employees, and therefore, generally unlawful. The processing is also likely to involve profiling, and possibly, automated decision-making. Therefore, employers should refrain from the use of facial recognition technologies. There may be some fringe exceptions to this rule, but such scenarios cannot be used to invoke a general legitimation of the use of such technology[20].

5.7 Processing operations involving vehicles used by employees

Technologies that enable employers to monitor their vehicles have become widely adopted, particularly among organisations whose activities involve transport or have significant vehicle fleets.

Any employer using vehicle telematics will be collecting data about both the vehicle and the individual employee using that vehicle. This data can include not just the location of the vehicle (and, hence, the employee) collected by basic GPS tracking systems, but, depending on the technology, a wealth of other information including driving behaviour. Certain technologies can also enable continuous monitoring both of the vehicle and the driver (eg, event data recorders).

An employer might be obliged to install tracking technology in vehicles to demonstrate compliance with other legal obligations, e.g. to ensure the safety of employees who drive those vehicles. The employer may also have a legitimate interest in being able to locate the

[19] See the above referenced case of *Köpke v Germany*; additionally, it should also be noted that in some jurisdictions the installation of systems such as CCTV for the purpose of proving unlawful conduct has been ruled permissible; see the case of *Bershka* in the Constitutional Court of Spain.

[20] Moreover, under the GDPR, processing of biometric data for identification purposes must be based on an exception provided by Art. 9(2).

vehicles at any time. Even if employers would have a legitimate interest to achieve these purposes, it should first be assessed whether the processing for these purposes is necessary, and whether the actual implementation complies with the principles of proportionality and subsidiarity. Where private use of a professional vehicle is allowed, the most important measure an employer can take to ensure compliance with these principles is the offering of an opt-out: the employee in principle should have the option to temporarily turn off location tracking when special circumstances justify this turning off, such as a visit to a doctor. This way, the employee can on its own initiative protect certain location data as private. The employer must ensure that the collected data are not used for illegitimate further processing, such as the tracking and evaluation of employees.

The employer must also clearly inform the employees that a tracking device has been installed in a company vehicle that they are driving, and that their movements are being recorded whilst they are using that vehicle (and that, depending on the technology involved, their driving behaviour may also be recorded). Preferably such information should be displayed prominently in every car, within eyesight of the driver.

It is possible that employees may use company vehicles outside working hours, e.g. for personal use, depending on the specific policies governing the use of those vehicles. Given the sensitivity of location data, it is unlikely that there is a legal basis for monitoring the locations of employees' vehicles outside agreed working hours. However, should such a necessity exist, an implementation that would be proportionate to the risks should be considered. For example, this could mean that, in order to prevent car theft, the location of the car is not registered outside working hours, unless the vehicle leaves a widely defined circle (region or even country). In addition, the location would only be shown in a "break-the-glass" way—the employer would only activate the "visibility" of the location, accessing the data already stored by the system, when the vehicle leaves a predefined region..

As stated in the WP29 *Opinion 13/2011 on Geolocation services on smart mobile devices*[21]:

> "Vehicle tracking devices are not staff tracking devices. Their function is to track or monitor the location of the vehicles in which they are installed. Employers should not regard them as devices to track or monitor the behaviour or the whereabouts of drivers or other staff, for example by sending alerts in relation to speed of vehicle."

Further, as stated in the WP29 *Opinion 5/2005 on the use of location data with a view to providing value-added services*[22]:

> "Processing location data can be justified where it is done as part of monitoring the transport of people or goods or improving the distribution of resources for services in scattered locations (e.g. planning operations in real time), or where a security objective is being pursued in relation to the employee himself or to the goods or vehicles in his charge. Conversely, the Working Party considers data processing to be excessive where employees

[21] WP29, *Opinion 13/2011 on Geolocation services on smart mobile devices,* WP 185, 16 May 2011, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp185_en.pdf

[22] WP29, *Opinion 5/2005 on the use of location data with a view to providing value-added services,* WP 115, 25 November 2005, url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf

are free to organise their travel arrangements as they wish or where it is done for the sole purpose of monitoring an employee's work where this can be monitored by other means."

5.7.1 EVENT DATA RECORDERS

Event data recorders provide an employer with the technical capability of processing a significant amount of personal data about the employees that drive company vehicles. Such devices are increasingly being placed into vehicles with the goal to record video, possibly including sound, in case of an accident. These systems are able to record at certain times, e.g. in response to sudden braking, abrupt directional change or accidents, where the moments immediately preceding the incident are stored, but they can also be set to monitor continuously. This information can be used subsequently to observe and review an individual's driving behaviour with the aim of improving it. Moreover, many of these systems include GPS to track the location of the vehicle in real-time and other details corresponding to the driving (such as the vehicle speed) can be also stored for further processing.

These devices have become particularly prevalent among organisations whose activities involve transport or have significant vehicle fleets. However, the deployment of event data recorders can only be lawful if there is a necessity to process the ensuing personal data about the employee for a legitimate purpose, and the processing complies with the principles of proportionality and subsidiarity.

Example

A transport company equips all of its vehicles with a video camera inside the cabin which records sound and video. The purpose of processing these data is to improve the driving skills of the employees. The cameras are configured to retain recordings whenever incidents such as sudden braking or abrupt directional change take place. The company assumes it has a legal ground for the processing in its legitimate interest under Article 7(f) of the Directive, to protect the safety of its employees and other drivers' safety.

However, the legitimate interest of the company to monitor the drivers does not prevail over the rights of those drivers to the protection of their personal data. The continuous monitoring of employees with such cameras constitutes a serious interference with their right of privacy. There are other methods (e.g., the installation of equipment that prevents the use of mobile phones) as well as other safety systems like an advanced emergency braking system or a lane departure warning system that can be used for the prevention of vehicle accidents which may be more appropriate. Furthermore, such a video has a high probability of resulting in the processing of personal data of third parties (such as pedestrians) and, for such a processing, the legitimate interest of the company is not sufficient to justify the processing.

5.8 Processing operations involving disclosure of employee data to third parties

It has become increasingly common for companies to transmit their employees' data to their customers for the purpose of ensuring reliable service provision. These data may be quite excessive depending on the scope of services provided (e.g. an employee's photo may be included). However, employees are not in a position, given the imbalance of power, to give free consent to the processing of their personal data by their employer, and if the data processing is not proportional, the employer does not have a legal ground.

Example:

A delivery company sends its customers an e-mail with a link to the name and the location of the deliverer (employee). The company also intended to provide a passport photo of the deliverer. The company assumed it would have a legal ground for the processing in its legitimate interest (Article 7(f) of the Directive), allowing the customer to check if the deliverer is indeed the right person.

However, it is not necessary to provide the name and the photo of the deliverer to the customers. Since there is no other legitimate ground for this processing, the delivery company is not allowed to provide these personal data to customers.

5.9 Processing operations involving international transfers of HR and other employee data

Employers are increasingly using cloud-based applications and services, such as those designed for the handling of HR-data as well as online office applications. The use of most of these applications will result in the international transfer of data from and concerning employees. As previously outlined in Opinion 08/2001, Art. 25 of the Directive states that transfers of personal data to a third country outside the EU can take place only where that country ensures an adequate level of protection. Whatever the basis, the transfer should satisfy the provisions of the Directive.

It should thus be ensured that these provisions concerning the international transfer of data are complied with. WP29 re-states its previous position that it is preferable to rely on adequate protection rather than the derogations listed in Art. 26 of the DPD; where consent is relied on it must be specific, unambiguous and freely-given. However, it should also be ensured that the data shared outside the EU/EEA, and subsequent access by other entities within the group, remains limited to the minimum necessary for the intended purposes.

6. Conclusions and Recommendations

6.1 Fundamental rights

The contents of communications above, as well as the traffic data relating to those communications, enjoy the same fundamental rights protections as “analogue” communications.

Electronic communications made from business premises may be covered by the notions of “private life” and “correspondence” within the meaning of Article 8 paragraph 1 of the European Convention. Based on the current Data Protection Directive employers may only collect the data for legitimate purposes, with the processing taking place under appropriate conditions (e.g., proportionate and necessary, for a real and present interest, in a lawful, articulated and transparent manner), with a legal basis for the processing of personal data collected from or generated through electronic communications.

The fact that an employer has the ownership of the electronic means does not rule out the right of employees to secrecy of their communications, related location data and correspondence. The tracking of the location of employees through their self-owned or company issued devices should be limited to where it is strictly necessary for a legitimate

purpose. Certainly, in the case of Bring Your Own Device it is important that employees are given the opportunity to shield their private communications from any work-related monitoring.

6.2 Consent; legitimate interest

Employees are almost never in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship. Given the imbalance of power, employees can only give free consent in exceptional circumstances, when no consequences at all are connected to acceptance or rejection of an offer.

The legitimate interest of employers can sometimes be invoked as a legal ground, but only if the processing is strictly necessary for a legitimate purpose and the processing complies with the principles of proportionality and subsidiarity. A proportionality test should be conducted prior to the deployment of any monitoring tool to consider whether all data are necessary, whether this processing outweighs the general privacy rights that employees also have in the workplace and what measures must be taken to ensure that infringements on the right to private life and the right to secrecy of communications are limited to the minimum necessary.

6.3 Transparency

Effective communication should be provided to employees concerning any monitoring that takes place, the purposes for this monitoring and the circumstances, as well as possibilities for employees to prevent their data being captured by monitoring technologies. Policies and rules concerning legitimate monitoring must be clear and readily accessible. The Working Party recommends involving a representative sample of employees in the creation and evaluation of such rules and policies as most monitoring has the potential to infringe on the private lives of employees.

6.4 Proportionality and data minimisation

Data processing at work must be a proportionate response to the risks faced by an employer. For example, internet misuse can be detected without the necessity of analysing website content. If misuse can be prevented (e.g., by using web filters) the employer has no general right to monitor.

Further, a blanket ban on communication for personal reasons is impractical and enforcement may require a level of monitoring that may be disproportionate. Prevention should be given much more weight than detection--the interests of the employer are better served by preventing internet misuse through technical means than by expending resources in detecting misuse.

The information registered from the ongoing monitoring, as well as the information that is shown to the employer, should be minimized as much as possible. Employees should have the possibility to temporarily shut off location tracking, if justified by the circumstances. Solutions that for example track vehicles can be designed to register the position data without presenting it to the employer.

Employers must take the principle of data minimisation into account when deciding on the deployment of new technologies. The information should be stored for the minimum amount

of time needed with a retention period specified. Whenever information is no longer needed it should be deleted.

6.5 Cloud services, online applications and international transfers

Where employees are expected to use online applications which process personal data (such as online office applications), employers should consider enabling employees to designate certain private spaces to which the employer may not gain access under any circumstances, such as a private mail or document folder.

The use of most applications in the cloud will result in the international transfer of employee data. It should be ensured that personal data transferred to a third country outside the EU takes place only where an adequate level of protection is ensured and that the data shared outside the EU/EEA and subsequent access by other entities within the group remains limited to the minimum necessary for the intended purposes.

* * *

Done in Brussels, on 8 June 2017

For the Working Party,
The Chairwoman
Isabelle FALQUE-PIERROTIN