

## Περιγραφή Υπηρεσιών Cloud της IBM

### IBM Digital Data Exchange

Ακολουθεί η Περιγραφή Υπηρεσιών για την Παραγγελία σας:

#### 1. Υπηρεσία Cloud

Η προσφορά Υπηρεσίας Cloud, συμπεριλαμβανομένης της βασικής προσφοράς και των διαθέσιμων προαιρετικών λειτουργιών, περιγράφεται παρακάτω και οι επιλογές σας προσδιορίζονται σε ένα Έγγραφο Παραγγελίας. Το Έγγραφο Παραγγελίας θα αποτελείται από την παρεχόμενη Προσφορά Τιμής και την Απόδειξη Δικαιώματος (Proof of Entitlement - "PoE") που θα λάβετε από την IBM, στην οποία επιβεβαιώνονται η ημερομηνία έναρξης και η περίοδος ισχύος των Υπηρεσιών Cloud, καθώς και η ημερομηνία έναρξης της τιμολόγησης.

##### 1.1 IBM Digital Data Exchange

Το IBM Digital Data Exchange είναι μια λύση που σας παρέχει μια ενιαία διεπαφή για την παραμετροποίηση και υλοποίηση προσδιοριστικών (tags) ιστοσελίδων και σελίδων για φορητές συσκευές.

Το IBM Digital Data Exchange σας παρέχει τη δυνατότητα να διαχειρίζεστε την υλοποίηση προσδιοριστικών (tags) της IBM και Εμπορικών Συνεργατών της IBM σε μια ιστοσελίδα ή σελίδα για φορητές συσκευές του οργανισμού σας. Το περιβάλλον χρήστη του IBM Digital Data Exchange παρέχει τη δυνατότητα άμεσου ελέγχου της διαδικασίας δημιουργίας προσδιοριστικών, καθώς επιτρέπει στους χρήστες να ορίζουν προσδιοριστικά για σελίδες και ομάδες σελίδων βάσει ενός συνόλου κανόνων που καθορίζουν την εκτέλεση των προσδιοριστικών. Έχοντας αγοράσει το IBM Digital Data Exchange, σας παρέχεται η δυνατότητα διαχείρισης της τρέχουσας ή μιας προηγούμενης υλοποίησης προσδιοριστικών της IBM, προσδιοριστικών Εμπορικών Συνεργατών της IBM και προσαρμοσμένου κώδικα JavaScript ή υποκείμενου σε δικαιώματα πνευματικής ιδιοκτησίας κώδικα σε διαφορετικά περιβάλλοντα.

#### 2. Περιγραφή Ασφάλειας

##### 2.1 Πολιτικές Ασφάλειας

Η IBM διατηρεί πολιτικές προστασίας δεδομένων προσωπικού χαρακτήρα και ασφάλειας οι οποίες δημοσιεύονται και κοινοποιούνται στους υπαλλήλους της IBM. Η IBM απαιτεί την παρακολούθηση εκπαιδευτικών σεμιναρίων σε θέματα προστασίας δεδομένων προσωπικού χαρακτήρα και ασφάλειας από άτομα, παγκοσμίως, που παρέχουν υποστήριξη σε κέντρα πληροφοριακών συστημάτων της IBM και έχει συγκροτήσει μια ομάδα ασφάλειας που ασχολείται αποκλειστικά με την ασφάλεια πληροφοριών. Οι πολιτικές και τα πρότυπα ασφάλειας της IBM επανεξετάζονται και αξιολογούνται σε ετήσια βάση. Τυχόν περιστατικά ασφάλειας στην IBM αντιμετωπίζονται σύμφωνα με μια αναλυτική διαδικασία απόκρισης σε περιστατικά.

##### 2.2 Έλεγχος Πρόσβασης

Η IBM μεριμνά για το λογικό διαχωρισμό των δεδομένων των πελατών της. Τα δεδομένα κάθε πελάτη αποθηκεύονται σε ένα χωριστό σχήμα (schema) που έχει σχεδιαστεί έτσι ώστε να επιτρέπει την πρόσβαση στα δεδομένα μέσω της Υπηρεσίας Cloud ή με την εξαγωγή τους από τον πελάτη. Ένας καθορισμένος από τον πελάτη διαχειριστής ελέγχει και διαχειρίζεται την πρόσβαση στην Υπηρεσία Cloud και στα δεδομένα του πελάτη. Η IBM χρησιμοποιεί τεχνολογία ταυτοποίησης πολλαπλών παραγόντων (multi-factor authentication) και κρυπτογράφησης VPN Tunnel κατά την πρόσβαση σε συστήματα πελατών. Η πρόσβαση περιορίζεται στα άτομα εκείνα που πρέπει να έχουν τη δυνατότητα πρόσβασης για τη συντήρηση και διαχείριση της Υπηρεσίας Cloud και της αντίστοιχης υποδομής υλικού εξοπλισμού και λογισμικού σε κέντρα πληροφοριακών συστημάτων τρίτων. Η IBM χρησιμοποιεί τεχνολογία WIFI (επίσης γνωστή ως 802.11) για τη μετάδοση ροών δεδομένων που κρυπτογραφούνται σύμφωνα με το πρωτόκολλο WPA2 με χρήση του αλγορίθμου κρυπτογράφησης AES και παρέχει για μη μεταδιδόμενες ταυτότητες SSID και αμοιβαία ταυτοποίηση μεταξύ του εξυπηρετητή και των τελικών συσκευών κατά την πρόσβαση σε συστήματα που περιέχουν δεδομένα πελατών.

##### 2.3 Ακεραιότητα και Διαθεσιμότητα Υπηρεσιών

Οι τροποποιήσεις στους πόρους λειτουργικού συστήματος (OSR) και στο λογισμικό εφαρμογών υπόκεινται στη διαδικασία διαχείρισης αλλαγών της IBM. Στην υποδομή δικτύου και στους σταθμούς εργασίας των ατόμων που εργάζονται στα κέντρα πληροφοριακών συστημάτων της IBM ή εργάζονται με

δεδομένα πελατών στα κέντρα πληροφοριακών συστημάτων της IBM χρησιμοποιούνται μηχανισμοί ελέγχου υλικού εξοπλισμού, λογισμικού, αρχείων καταγραφής πρόσβασης (access logs), πρόσβασης για ανάγνωση μόνο (read only access) και κρυπτογράφησης προκειμένου να ελαχιστοποιείται η πιθανότητα μετάδοσης και εκτέλεσης ιών (computer virus) και άλλων γνωστών μορφών επιβλαβούς κώδικα. IBM κρυπτογραφεί τα δεδομένα που μεταδίδονται μέσω του δικτύου χρησιμοποιώντας τυπικές συνδέσεις SSL (https), ενώ η υποδομή δικτύου της IBM χρησιμοποιεί τεχνολογικές λύσεις διατεμαχικής (end-to-end) ασφάλειας, συμπεριλαμβανομένων τεχνολογιών τείχους προστασίας (firewall), αποτροπής μη εξουσιοδοτημένης πρόσβασης και αντιμετώπισης επιβλαβούς κώδικα. Διεξάγονται περιοδικοί έλεγχοι για τρωτά σημεία στην υποδομή TCP/IP (Transmission Control Protocols/Internet Protocols) από εξουσιοδοτημένους διαχειριστές για τον εντοπισμό και επίλυση δυνητικών περιπτώσεων έκθεσης συστημάτων σε κινδύνους. Τα δεδομένα αντιγράφονται από το data warehouse της IBM σε δευτερεύοντα αποθηκευτικά μέσα στο κέντρο πληροφοριακών συστημάτων, ενώ δημιουργούνται διπλότυπα κρυπτογραφημένα αντίγραφα για τριτοβάθμια αρχειοθέτηση (σε ταινία) σε κάποιο κέντρο αποκατάστασης μετά από καταστροφή που ανήκει σε τρίτη εταιρεία, εκτός των εγκαταστάσεων IBM.

## 2.4 Καταγραφή Δραστηριότητας

Η IBM τηρεί αρχεία καταγραφής των δραστηριοτήτων της για συστήματα, εφαρμογές, χώρους αποθήκευσης δεδομένων (data repositories), middleware και συσκευές υποδομής δικτύου που υποστηρίζουν και έχουν παραμετροποιηθεί για την καταγραφή δραστηριότητας. Η IBM τηρεί αρχεία καταγραφής (logs) στα οποία καταγράφονται i) επιτυχείς και ανεπιτυχείς προσπάθειες σύνδεσης χρηστών, ii) επιτυχείς και ανεπιτυχείς προσπάθειες απόκτησης πρόσβασης στην υποδομή από κάποια εξωτερική τοποθεσία, iii) προσπάθειες ενημέρωσης πόρων του λειτουργικού συστήματος (OSR), και iv) δραστηριότητες ατόμων που διαθέτουν εξουσιοδότηση διαχείρισης συστήματος ή διαχείρισης ασφάλειας.

## 2.5 Φυσική Ασφάλεια

Η IBM περιορίζει την πρόσβαση αποκλειστικά σε εξουσιοδοτημένο προσωπικό των κέντρων πληροφοριακών συστημάτων της IBM εντός των εγκαταστάσεων της IBM και των κέντρων πληροφοριακών συστημάτων της IBM που παρέχονται από τρίτες εταιρείες. Το περιβάλλον της Υπηρεσίας Cloud της IBM περιλαμβάνει ταυτοποίηση πολλαπλών παραγόντων (multi-factor authentication) για τον έλεγχο της φυσικής πρόσβασης, με την εισαγωγή ενός μοναδικού κωδικού και με σάρωση βιομετρικών στοιχείων, καθώς και 24x7 παρουσία προσωπικού ασφάλειας, επανδρωμένη ασφάλεια και παρακολούθηση με βιντεοκάμερες. Η IBM αποτρέπει την μη εξουσιοδοτημένη προβολή, αντιγραφή, τροποποίηση ή αφαίρεση οποιωνδήποτε αποθηκευτικών μέσων στα οποία περιλαμβάνονται δεδομένα πελατών. Τα αφαιρούμενα μέσα στα οποία αποθηκεύονται δεδομένα πελατών (συμπεριλαμβανομένων συσκευών αποθήκευσης USB, CD και DVD) κρυπτογραφούνται με αλγόριθμους κρυπτογράφησης τουλάχιστον 256-bit AES (ή ισοδύναμη κρυπτογράφηση). Στους παρεχόμενους από την IBM φορητούς υπολογιστές και σταθμούς εργασίας απαιτείται η εφαρμογή τεχνολογίας κρυπτογράφησης ολόκληρου του δίσκου (PGP) στις περιπτώσεις όπου ενδέχεται να είναι απαραίτητο να χορηγηθούν στον κάτοχο του υπολογιστή δικαιώματα πρόσβασης σε ευαίσθητα δεδομένα ή δεδομένα πελατών. Η IBM καταστρέφει τα αφαιρούμενα μέσα αποθήκευσης και οποιεσδήποτε φορητές συσκευές (όπως π.χ. οπτικοί δίσκοι, μονάδες USB, DVD, ταινίες εφεδρικής αποθήκευσης, εκτυπωτές και φορητοί υπολογιστές) που περιέχουν δεδομένα πελατών, ή καθιστά τα δεδομένα πελατών στα εν λόγω φυσικά μέσα μη αναγνώσιμα και μη ανακατασκευάσιμα με οποιαδήποτε τεχνικά μέσα, προτού προβεί στην επαναχρησιμοποίηση των εν λόγω μέσων. Η IBM επεξεργάζεται τα απορρίμματα χαρτιού της με τη χρήση καταστροφέα χαρτιού (shredder) και τα απορρίπτει με ασφαλή και εμπιστευτικό τρόπο έτσι ώστε να μην είναι δυνατή η ανάγνωση των εν λόγω απορριμμάτων χαρτιού.

## 2.6 Συμμόρφωση

Η IBM πιστοποιεί σε ετήσια βάση τη συμμόρφωση των δικών της πρακτικών προστασίας δεδομένων προσωπικού χαρακτήρα με τις Αρχές του Πλαισίου Αρχών Safe Harbor ("Ασφαλής Λιμένας") του Υπουργείου Εμπορίου των Η.Π.Α.: Notice (Ειδοποίηση), Choice (Επιλογή), Onward Transfer (Διαβίβαση), Access and Accuracy (Πρόσβαση και Ακρίβεια), Security (Ασφάλεια) και Oversight/Enforcement (Εποπτεία/Επιβολή). Σε ετήσια βάση διεξάγεται πρότυπος έλεγχος (audit) SSAE 16 Type (παλιότερα SAS 70), ή ισοδύναμος έλεγχος, στα κέντρα πληροφοριακών συστημάτων του περιβάλλοντος παραγωγής μας. Η IBM ελέγχει τη συμμόρφωση των δραστηριοτήτων της στον τομέα της ασφάλειας και της προστασίας δεδομένων προσωπικού χαρακτήρα με τις επιχειρηματικές της απαιτήσεις. Σε τακτική βάση διεξάγονται αξιολογήσεις και έλεγχοι από την IBM προκειμένου να επιβεβαιώνεται η συμμόρφωση με τις πολιτικές ασφάλειας πληροφοριών της. Οι εφαρμοζόμενες πολιτικές ασφάλειας προβλέπουν τη διεξαγωγή ελέγχων ασφάλειας, την περιοδική εφαρμογή επιδιορθώσεων ασφάλειας και τη διαχείριση και τον έλεγχο κωδικών πρόσβασης. Σε ετήσια βάση οι υπάλληλοι της IBM και των προμηθευτών της παρακολουθούν ένα σεμινάριο εκπαίδευσης και ευαισθητοποίησης εργατικού δυναμικού σε θέματα ασφάλειας. Στα μέλη του προσωπικού υπενθυμίζονται σε ετήσια βάση οι στόχοι

που σχετίζονται με την επαγγελματική τους θέση και οι υποχρεώσεις τους αναφορικά με την ηθική επιχειρηματική συμπεριφορά, την τήρηση εμπιστευτικότητας και την ασφάλεια της IBM.

### 3. Στόχοι για το Επίπεδο Παροχής Υπηρεσιών

Στόχος της IBM είναι να καθιστά την Υπηρεσία Cloud διαθέσιμη στον Πελάτη με ποσοστό διαθεσιμότητας 99%. Οι Στόχοι για το Επίπεδο Παροχής Υπηρεσιών δεν αποτελούν συμβατική δέσμευση αλλά ένα σύνολο στόχων στους οποίους η ομάδα Υποστήριξης Πελατών της IBM επιδιώκει να ανταποκρίνεται ή να υπερβαίνει δια μέσου των διαδικασιών, της τεχνολογίας και των στελεχών της.

## 4. Δικαιώματα και Τιμολόγηση

### 4.1 Μετρικά Συστήματα Χρέωσης

Η Υπηρεσία Cloud καθίσταται διαθέσιμη βάσει ενός των παρακάτω μετρικών συστημάτων χρέωσης, όπως καθορίζεται στο Έγγραφο Συναλλαγής:

- α. Εκατομμύριο Κλήσεις στον Εξυπηρετητή (Million Server Calls - MSC) είναι μια μονάδα μέτρησης βάσει της οποίας μπορεί να αποκτηθεί η Υπηρεσία Cloud. Κλήση στον Εξυπηρετητή είναι δεδομένα που διαβιβάζονται στην Υπηρεσία Cloud και τα οποία επεξεργάζεται η Υπηρεσία Cloud ως αποτέλεσμα ενός προσδιορισμένου συμβάντος, το οποίο προκλήθηκε από έναν παρακολουθούμενο επισκέπτη για ένα Entity ID ("Ταυτότητα Οντότητας"). Μια Κλήση στον Εξυπηρετητή της οποίας γίνεται επεξεργασία από διαφορετικά Entity IDs θα μετράται ως μία μοναδική Κλήση στον Εξυπηρετητή για κάθε μοναδικό Entity ID. Ένα Entity ID διαχωρίζει ή/και ελέγχει δικαιώματα πρόσβασης σε δεδομένα στην Υπηρεσία Cloud, στα οποία μπορεί να περιλαμβάνονται επεξεργασμένα δεδομένα από έναν ή περισσότερους δικτυακούς τόπους σας. Κάθε Δικαίωμα MSC αντιπροσωπεύει ένα Εκατομμύριο Κλήσεις στον Εξυπηρετητή. Πρέπει να αποκτηθούν επαρκή δικαιώματα MSC για την κάλυψη του αριθμού κλήσεων στον Εξυπηρετητή των οποίων γίνεται επεξεργασία κατά τη διάρκεια της περιόδου μέτρησης που καθορίζεται στο Έγγραφο Παραγγελίας.

### 4.2 Χρεώσεις και Τιμολόγηση

Το πληρωτέο ποσό για την Υπηρεσία Cloud καθορίζεται στο Έγγραφο Παραγγελίας.

## 5. Περίοδος Ισχύος και Επιλογές Ανανέωσης

### 5.1 Περίοδος Ισχύος

Η περίοδος ισχύος της Υπηρεσίας Cloud αρχίζει κατά την ημερομηνία που η IBM σας ειδοποιεί ότι έχετε πρόσβαση στην Υπηρεσία Cloud, όπως περιγράφεται στο Έγγραφο Παραγγελίας. Στο τμήμα της Απόδειξης Δικαιώματος στο Έγγραφο Παραγγελίας θα επιβεβαιώνονται οι ακριβείς ημερομηνίες έναρξης και λήξης της περιόδου ισχύος. Επιτρέπεται να αυξήσετε το δικό σας επίπεδο χρήσης της Υπηρεσίας Cloud κατά τη διάρκεια της περιόδου ισχύος κατόπιν σχετικής επικοινωνίας με την IBM ή έναν Εμπορικό Συνεργάτη της IBM. Θα επιβεβαιώσουμε το αυξημένο επίπεδο χρήσης στο Έγγραφο Παραγγελίας.

### 5.2 Επιλογές Ανανέωσης Περιόδου Ισχύος Υπηρεσιών Cloud

Στο Έγγραφο Παραγγελίας σας θα καθορίζεται αν η Υπηρεσία Cloud θα ανανεώνεται με τη λήξη της περιόδου ισχύος, ορίζοντας την περίοδο ισχύος ως μία από τις ακόλουθες:

#### 5.2.1 Αυτόματη Ανανέωση

Εάν στο Έγγραφο Παραγγελίας σας ορίζεται ότι η ανανέωση της περιόδου ισχύος γίνεται αυτόματα, μπορείτε να καταργήσετε τη λήγουσα Υπηρεσία Cloud με έγγραφο αίτημα, τουλάχιστον ενενήντα (90) ημέρες πριν την ημερομηνία λήξης της περιόδου ισχύος που καθορίζεται στο Έγγραφο Παραγγελίας. Εάν η IBM ή ο Εμπορικός Συνεργάτης της IBM που σας εξυπηρετεί δεν έχει λάβει τέτοια ειδοποίηση διακοπής πριν την ημερομηνία λήξης, η λήγουσα περίοδος ισχύος ανανεώνεται αυτόματα είτε για περίοδο ενός έτους είτε για χρονική περίοδο με την ίδια διάρκεια με την αρχική περίοδο ισχύος που καθορίζεται στην Απόδειξη Δικαιώματος.

#### 5.2.2 Συνεχόμενη Τιμολόγηση

Όταν στο Έγγραφο Παραγγελίας σας δηλώνεται ότι γίνεται συνεχόμενη τιμολόγηση, θα εξακολουθείτε να έχετε πρόσβαση στην Υπηρεσία Cloud και θα τιμολογείστε για τη χρήση της Υπηρεσίας Cloud σε συνεχή βάση. Για να διακόψετε τη χρήση της Υπηρεσίας Cloud και τη διαδικασία συνεχόμενης τιμολόγησης, θα πρέπει να παράσχετε στην IBM ή στον Εμπορικό Συνεργάτη της IBM που σας εξυπηρετεί έγγραφο ειδοποίηση ενενήντα (90) ημερών στην οποία ζητάτε την ακύρωση της Υπηρεσίας Cloud σας. Μετά την ακύρωση της πρόσβασής σας, θα τιμολογηθείτε για οποιοσδήποτε εκκρεμείς χρεώσεις πρόσβασης έως το μήνα κατά τον οποίο τέθηκε σε ισχύ η ακύρωση.

### 5.2.3 Απαιτείται Ανανέωση

Όταν στο Έγγραφο Παραγγελίας σας δηλώνεται ότι το είδος ανανέωσης είναι "λήξη", η Υπηρεσία Cloud θα τερματιστεί με τη λήξη της περιόδου ισχύος και η πρόσβασή σας στην Υπηρεσία Cloud θα καταργηθεί. Για να συνεχίσετε να χρησιμοποιείτε την Υπηρεσία Cloud μετά την ημερομηνία λήξης, θα πρέπει να υποβάλετε μια παραγγελία στον εκπρόσωπο πωλήσεων της IBM ή σε έναν Εμπορικό Συνεργάτη της IBM προκειμένου να αγοράσετε μια νέα περίοδο συνδρομής.

## 6. Τεχνική Υποστήριξη

Παρέχεται τεχνική υποστήριξη για την Υπηρεσία Cloud και το Λογισμικό Ενεργοποίησης, ανάλογα με την περίπτωση, κατά τη διάρκεια της Περιόδου Συνδρομής. Η εν λόγω τεχνική υποστήριξη περιλαμβάνεται στην Υπηρεσία Cloud και δεν διατίθεται ως χωριστή προσφορά.

Στην ακόλουθη ιστοσελίδα παρέχονται περισσότερες πληροφορίες για την Τεχνική Υποστήριξη:  
[http://www-01.ibm.com/software/support/acceleratedvalue/SaaS\\_Handbook\\_V18.pdf](http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf).

## 7. Λογισμικό Ενεργοποίησης

- α. Αυτή η προσφορά Υπηρεσίας Cloud μπορεί να περιλαμβάνει λογισμικό ενεργοποίησης. Επιτρέπεται να χρησιμοποιήσετε το λογισμικό ενεργοποίησης μόνο στα πλαίσια της εκ μέρους σας χρήσης της Υπηρεσίας Cloud, για τη διάρκεια της περιόδου ισχύος της Υπηρεσίας Cloud. Στο βαθμό που το λογισμικό ενεργοποίησης περιλαμβάνει δείγματα κώδικα, διαθέτετε το πρόσθετο δικαίωμα να δημιουργήσετε παράγωγα έργα των δειγμάτων κώδικα και να τα χρησιμοποιείτε με τρόπο που να είναι συμβατό με την παρούσα άδεια. Το λογισμικό ενεργοποίησης παρέχεται βάσει της Σύμβασης SLA, εάν υπάρχει, ως τμήμα της Υπηρεσίας Cloud, αλλά άλλως παρέχεται "ΩΣ ΕΧΕΙ", χωρίς εγγύηση.

## 8. Πρόσθετες Πληροφορίες

### 8.1 Λεπτομέρειες Δικαιωμάτων

Στη χρέωση συνδρομής για το IBM Digital Data Exchange περιλαμβάνονται τα εξής:

- α. Θα λάβετε μία περίπτωση χρήσης (instance) του IBM Digital Data Exchange.
- β. Βασική παροχή έως πέντε (5) εξ αποστάσεως υπηρεσιών υλοποίησης για την αρχική σας εξοικείωση (onboarding) με το IBM Digital Data Exchange. Οι υπηρεσίες λήγουν 90 ημέρες από την ημερομηνία κατά την οποία ειδοποιείστε από την IBM ότι η πρόσβασή σας στην Υπηρεσία Cloud είναι διαθέσιμη, ανεξάρτητα από το εάν έχουν χρησιμοποιηθεί όλες οι ώρες.

### 8.2 Ειδοποίηση και Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

Συμφωνείτε (i) να παρέχετε μια σαφή και ευδιάκριτη διασύνδεση (link) προς τους όρους χρήσης του δικτυακού τόπου σας και την πολιτική προστασίας δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένης μιας διασύνδεσης προς τις πρακτικές συλλογής και χρήσης δεδομένων της IBM (<http://www.ibm.com/software/marketing-solutions/privacy/index.html>) και της εταιρείας ή του οργανισμού σας, (ii) να παρέχετε ειδοποίηση ότι τοποθετούνται cookies και αρχεία τύπου clear gif/web beacon στον υπολογιστή του επισκέπτη από την IBM για λογαριασμό σας, μαζί με μια εξήγηση του σκοπού και της χρήσης της εν λόγω τεχνολογίας, και (iii) στο βαθμό που απαιτείται από το νόμο, να αποκτάτε τη συναίνεση των επισκεπτών του δικτυακού τόπου πριν την τοποθέτηση cookies και αρχείων τύπου clear gif/web beacon από εσάς ή την IBM για λογαριασμό σας σε συσκευές των εν λόγω επισκεπτών.

Είστε ενήμεροι και συμφωνείτε ότι η IBM μπορεί, στα πλαίσια της κανονικής λειτουργίας και υποστήριξης των Υπηρεσιών Cloud, να προβαίνει στη συλλογή δεδομένων προσωπικού χαρακτήρα σας (των υπαλλήλων και των εργαζομένων σας) σχετικά με τη χρήση των Υπηρεσιών Cloud, μέσω τεχνολογιών παρακολούθησης και άλλων τεχνολογιών. Με αυτό τον τρόπο η IBM συγκεντρώνει στατιστικά στοιχεία χρήσης και πληροφορίες για την αποτελεσματικότητα των Υπηρεσιών Cloud με σκοπό τη βελτίωση της γενικής εμπειρίας των χρηστών ή/και την εξατομικευμένη αλληλεπίδραση μαζί σας. Επιβεβαιώνετε ότι θα αποκτήσετε ή έχετε αποκτήσει την απαιτούμενη συναίνεση προκειμένου η IBM να προβεί στην επεξεργασία δεδομένων προσωπικού χαρακτήρα για τον ανωτέρω σκοπό εντός της IBM, άλλων εταιρειών IBM και των υπεργολάβων της, οπουδήποτε δραστηριοποιούμαστε επιχειρηματικά, συμμορφούμενοι με το εφαρμοστέο δίκαιο. Η IBM θα ανταποκρίνεται στα αιτήματα των υπαλλήλων και υπεργολάβων σας αναφορικά με την πρόσβαση, ενημέρωση, διόρθωση ή διαγραφή των συλλεχθέντων δεδομένων προσωπικού χαρακτήρα τους.

### 8.3 Τοποθεσίες Αντλούμενων Οφελών

Κατά περίπτωση, οι φόροι βασίζονται στην τοποθεσία ή στις τοποθεσίες που προσδιορίζετε ως αντλούσες οφέλη των Υπηρεσιών Cloud. Η IBM θα εφαρμόζει φόρους με βάση την επαγγελματική διεύθυνση που δηλώνεται κατά την παραγγελία μιας Υπηρεσίας Cloud ως κύρια επωφελούμενη

τοποθεσία, εκτός εάν παράσχετε πρόσθετες πληροφορίες στην IBM. Εσείς είστε υπεύθυνοι για την έγκαιρη ενημέρωση των εν λόγω πληροφοριών και την κοινοποίηση οποιωνδήποτε αλλαγών στην IBM.