

## IBM Cloud Integrated Analytics Environment

Termenii de Utilizare ("TdU") sunt alcătuiți din acești Termeni de Utilizare IBM – Termeni Specifici Ofertei SaaS ("Termenii Specifici Ofertei SaaS") și un document intitulat Termenii de Utilizare IBM – Termeni Generali ("Termenii Generali"), disponibil la următorul URL: <http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/>.

În eventualitatea unui conflict, Termenii Specifici Ofertei SaaS vor prevala față de Termenii Generali. Prin comandarea, accesarea sau utilizarea IBM SaaS, Clientul este de acord cu Termenii de Utilizare.

Termenii de Utilizare sunt guvernați de IBM International Passport Advantage Agreement, IBM International Passport Advantage Express Agreement sau IBM International Agreement for Selected IBM SaaS Offerings, după caz ("Contractul"), care împreună cu Termenii de Utilizare reprezintă acordul complet.

### 1. IBM SaaS

Acești Termeni Specifici Ofertei SaaS acoperă următoarele oferte IBM SaaS:

- IBM Cloud Integrated Analytics Environment
- IBM Cloud Integrated Analytics VPN Connectivity
- IBM Cloud Integrated Analytics Standard Security Appliance
- IBM Cloud Integrated Analytics Enterprise Security Appliance
- IBM Cloud Integrated Analytics Extra Small Server
- IBM Cloud Integrated Analytics Small Server
- IBM Cloud Integrated Analytics Medium Server
- IBM Cloud Integrated Analytics Large Server
- IBM Cloud Integrated Analytics SAN Storage

### 2. Indicii de Măsurare pentru Tarifare

IBM SaaS este vândut în baza unuia dintre următorii indici de măsurare pentru tarifare, după cum este specificat în Documentul Tranzacțional:

- Instanță** – este o unitate de măsură pentru obținerea IBM SaaS. O Instanță este accesul la o configurație IBM SaaS specifică. Trebuie obținute drepturi suficiente pentru fiecare Instanță a IBM SaaS făcută disponibilă pentru acces și utilizare pe durata perioadei de măsurare specificate în Dovada Dreptului de Utilizare (Proof of Entitlement - PoE) sau Documentul Tranzacțional al Clientului.
- Gigabyte** – este o unitate de măsură pentru obținerea IBM SaaS. Un Gigabyte este definit ca 2 la puterea 30 de byți de date (1.073.741.824 byți). Trebuie obținute drepturi suficiente pentru a acoperi numărul total de Gigabytes procesați de IBM SaaS pe durata perioadei de măsurare specificate în Dovada Dreptului de Utilizare (Proof of Entitlement - PoE) sau Documentul Tranzacțional al Clientului.

### 3. Tarife și Facturare

Suma de plată pentru IBM SaaS este specificată într-un Document Tranzacțional.

#### 3.1 Tarife Lunare Parțiale

Un tarif lunar parțial, după cum este specificat în Documentul Tranzacțional, poate fi evaluat prin proratare.

### 4. Opțiunile pentru Termen și Reînnoire

Termenul IBM SaaS începe la data la care IBM anunță Clientul că acesta are acces la IBM SaaS, după cum este specificat în PoE. Dovada Dreptului de Utilizare (PoE) va specifica dacă oferta IBM SaaS este reînnoită automat, va fi furnizată mai departe pe bază de utilizare continuă sau se va termina la sfârșitul termenului.

În cazul reînnoirii automate, cu excepția situației în care Clientul, cu cel puțin 90 de zile înainte de expirarea termenului, trimite o notificare scrisă prin care anunță că nu dorește reînnoirea, oferta IBM SaaS va fi reînnoită automat pentru termenul specificat în PoE.

În cazul utilizării continue, oferta IBM SaaS va continua să fie disponibilă, de la lună la lună, până când Clientul trimite, cu 90 de zile înainte, o notificare scrisă privind terminarea. După această perioadă de 90 de zile, oferta IBM SaaS va rămâne disponibilă până la sfârșitul lunii calendaristice.

## 5. Suport Tehnic

Suportul tehnic pentru IBM SaaS este furnizat prin forumuri online și un sistem de raportare a problemelor online. IBM va face disponibilă publicația IBM Software as a Service Support Handbook, care conține informații privind contactarea suportului tehnic și alte informații și procese. Suportul Tehnic este furnizat cu IBM SaaS și nu este disponibil ca ofertă separată.

Severitate	Definiție Severitate	Obiective Timp de Răspuns	Acoperire Timp de Răspuns
1	<b>Impact critic asupra afacerii/serviciu întrerupt:</b> O funcționalitate cu caracter critic pentru afacere este inoperabilă sau o interfață cu caracter critic nu funcționează. De obicei aceasta se aplică în cazul unui mediu de producție și indică incapacitatea de a accesa serviciile, ceea ce are un impact critic asupra operațiilor. Această condiție necesită o soluționare imediată.	Într-un interval de 1 oră	24x7
2	<b>Impact semnificativ asupra afacerii:</b> O caracteristică sau o funcție a serviciului a suferit o restricție importantă privind utilizarea sau Clientul nu poate îndeplini termenele limită ale afacerii.	Într-un interval de 2 ore de lucru	Orele de lucru L-V
3	<b>Impact minor asupra afacerii:</b> Indică situația în care serviciul sau funcționalitatea permite utilizarea și nu are un impact critic asupra operațiilor.	Într-un interval de 4 ore de lucru	Orele de lucru L-V
4	<b>Impact minim asupra afacerii:</b> O întrebare sau o cerere care nu are caracter tehnic.	Într-un interval de 1 zi lucrătoare	Orele de lucru L-V

## 6. Termeni Suplimentari pentru Oferta IBM SaaS

### 6.1 General

Clientul este de acord ca IBM să poată face referire în mod public la Client ca abonat al IBM SaaS, într-un comunicat de presă sau de marketing.

### 6.2 Locații de Beneficiu Derivate

Când este aplicabil, taxele sunt bazate pe locațiile pe care Clientul le identifică ca loc unde beneficiază de IBM SaaS. IBM va aplica taxele utilizând adresa de afaceri specificată ca locație principală de beneficiu, atunci când se comandă un IBM SaaS, cu excepția cazului în care IBM primește alte informații de la Client. Clientul este responsabil pentru păstrarea acestor informații și trimiterea oricărei modificări la IBM.

### 6.3 Descrierea Securității

Acest IBM SaaS respectă principiile IBM privind securitatea și confidențialitatea datelor pentru IBM SaaS, care sunt disponibile la <http://www.ibm.com/cloud/data-security>, și orice termeni suplimentari specificați în această secțiune. Nicio modificare a principiilor IBM privind securitatea și confidențialitatea datelor nu va afecta securitatea IBM SaaS.

IBM îi va furniza Clientului o notificare privind incidentele legate de securitate, însă Clientul este responsabil pentru investigarea și rezolvarea incidentelor respective. IBM își rezervă dreptul de a izola și suspenda IBM SaaS, dacă aceste este compromis ca urmare a unui incident nerezolvat.

Oferta IBM Cloud Integrated Analytics VPN Connectivity criptează conținutul pe durata transmiterii datelor între rețeaua IBM și rețeaua Clientului. IBM SaaS nu criptează conținutul static, când se așteaptă transmiterea de date. Clientul este responsabil pentru criptarea conținutului înainte de adăugarea în IBM SaaS.

### **6.3.1 Informații Personale și Date Reglementate**

Pentru ofertele implementate în Zona de Servicii Gestionate (conform definiției din Anexa A), Descrierea Serviciului sau Termenii de Utilizare pentru ofertele respective specifică cerințele de securitate pentru procesarea informațiilor personale și a datelor reglementate.

Pentru ofertele implementate în Zona Gestionată IBM SaaS nu este conceput pentru cerințele de securitate specifice conținutului reglementat, cum ar fi informațiile personale sau informațiile personale sensibile. Clientul este responsabil pentru a determina dacă acest IBM SaaS îndeplinește cerințele Clientului privind tipul de conținut pe care îl utilizează Clientul în legătură cu IBM SaaS.

### **6.3.2 Utilizarea Datelor Compilate**

IBM poate monitoriza utilizarea de către Client a IBM SaaS, în scopul cercetării interne IBM, testării și dezvoltării îmbunătățirilor pentru IBM SaaS, pentru dezvoltarea unor servicii noi sau furnizarea către Client a unor servicii suplimentare, care să le asigure utilizatorilor o experiență mai bine adaptată și mai semnificativă. Pentru a face aceasta, IBM poate compila și analiza, într-un format agregat și anonimizat, informații de sumar care reflectă utilizarea IBM SaaS de către utilizatorii autorizați ai Clientului și poate pregăti rapoarte, studii, analize și alte produse de lucru ce rezultă din respectivele compilări și analize (numite colectiv "Date Compilate"). IBM păstrează drepturile de proprietate privind Datele Compilate.

## **6.4 Obligațiile Clientului**

### **6.4.1 IBM Cloud Integrated Analytics VPN Connectivity**

- Completarea chestionarului Virtual Private Network ("VPN") și returnarea lui către IBM pentru examinare, înainte de data de început a configurării VPN.
- Furnizarea unui punct de contact tehnic unic, care cunoaște cerințele clientului legate de rețeaua companiei, VPN și securitate.
- Asigurarea că este disponibil un administrator de securitate și de rețea în timpul fazei de configurare și validare a configurației VPN, pentru a colabora cu IBM la finalizarea setării VPN.
- Asigurarea integrală a administrării, mentenanței, modificării, configurării și testării hardware-ului și software-ului, în locația clientului utilizată pentru VPN.
- Testarea acceptării de către utilizator, pentru validarea configurației VPN pe durata implementării.
- Notificarea, prin sistemul de raportare online a problemelor, a oricăror modificări necesare pentru configurația VPN.

## Anexa A

### 1. Descrierea IBM SaaS

IBM Cloud Integrated Analytics Environment (CIAE) este un model de implementare ce asigură conectivitatea privată, nativă, între oferte IBM SaaS activate diferit, cumpărate separat, precum și opțiuni pentru o conectivitate sigură a clientului. Principalele două categorii ale acestor oferte sunt:

- Oferte complet gestionate IBM Analytics (de exemplu, dashDB Enterprise, BigInsights on Cloud, Cognos BI etc.)
- Oferte găzduite IBM Analytics (de exemplu, DB2 on Cloud, Master Data Management on Cloud, DataStage on Cloud) și software gestionat de Client, implementat pe Servere ICIA.

IBM SaaS într-o zonă găzduită include:

- Notificarea incidentelor
- Gestionarea hardware-ului/infrastructurii, exceptând:
  - IBM Cloud Integrated Analytics Standard Security Appliance
  - IBM Cloud Integrated Analytics Enterprise Security Appliance
- Notificarea și rezolvarea problemelor la nivel fizic, pentru infrastructura gestionată IBM
- Securitatea facilității, controlul accesului și înregistrările de mentenanță
- Casarea și reutilizarea mediilor de stocare

Clientul trebuie să cumpere următoarele drepturi de utilizare:

- IBM Cloud Integrated Analytics Entitlement; și
- IBM Cloud Integrated Analytics VPN Connectivity, sau IBM Cloud Integrated Analytics Standard Security Appliance, sau IBM Cloud Integrated Analytics Enterprise Security Appliance.

Pentru scopurile documentului Data Security and Privacy Principles, oferta IBM SaaS este clasificată ca o ofertă Infrastructure as a Service (IaaS).

#### 1.1 IBM Cloud Integrated Analytics Environment

IBM Cloud Integrated Analytics Environment este implementat într-un centru de date IBM SoftLayer și constă în două zone:

- a. O Zonă de Servicii Gestionate, în care sunt implementate servicii gestionate native CIAE (inclusiv VPN-uri site-la-site gestionate de IBM), precum și oferte SaaS gestionate IBM Analytics. Această zonă este gestionată de IBM. Pentru scopurile documentului Data Security and Privacy Principles, porțiunea Zonă de Servicii Gestionate a ofertei este clasificată ca o ofertă Software as a Service (SaaS).
- b. O Zonă Găzduită, în care sunt implementate oferte SaaS găzduite IBM Analytics. Aceste sisteme pot fi:
  - Oferte găzduite, ca, de exemplu, DB2 on Cloud
  - Servere ICIA, după cum este definit mai jos.
  - Zona Găzduită este opțiunea de utilizare a unui firewall exterior, utilizând o ofertă IBM Cloud Integrated Analytics Standard Security Appliance sau IBM Cloud Integrated Analytics Enterprise Security Appliance, cumpărată separat și gestionată de Client.

#### 1.2 IBM Cloud Integrated Analytics VPN Connectivity

Serviciul VPN site-la-site gestionat de IBM. IBM va termina în mod automat fiecare conexiune VPN atunci când utilizarea IBM Cloud Integrated Analytics Environment a încetat. Serviciul IBM Cloud Integrated Analytics VPN Connectivity utilizează tehnologia VPN IPsec site-la-site.

#### 1.3 IBM Cloud Integrated Analytics Standard Security Appliance

Un dispozitiv de securitate implementat în Zona Găzduită și gestionat de Client. Este utilizat de Client pentru a activa un VPN site-la-site gestionat de Client sau un VPN client-la-site gestionat de Client, precum și pentru a utiliza un firewall pentru zona găzduită din spațiul Internet public.

## **1.4 IBM Cloud Integrated Analytics Enterprise Security Appliance**

O pereche de dispozitive de securitate redundante, implementate în Zona Găzduită și gestionate de Client, ce permite activarea unui VPN site-la-site gestionat de Client sau a unui VPN client-la-site gestionat de Client, precum și utilizarea unui firewall pentru zona găzduită din spațiul Internet public.

## **1.5 Servere ICIA**

Servere IBM Cloud Integrated Analytics Environment care sunt implementate în zona găzduită și sunt utilizate pentru aplicații deținute de Client, care necesită conectivitate cu viteză înaltă și latență redusă cu alte aplicații din Zona de Servicii Gestionate și Zona Găzduită.

### **1.5.1 IBM Cloud Integrated Analytics Extra Small Server**

Un server SoftLayer gestionat de Client, cu specificații minime de 1 nucleu virtual public, 4 GB RAM, disc SAN de 25 GB.

### **1.5.2 IBM Cloud Integrated Analytics Small Server**

Un server SoftLayer gestionat de Client, cu specificații minime de 4 nuclee virtuale private, 16 GB RAM, disc SAN de 100 GB.

### **1.5.3 IBM Cloud Integrated Analytics Medium Server**

Un server SoftLayer gestionat de Client, cu specificații minime de 8 nuclee virtuale private, 32 GB RAM, discul 1 SAN de 100 GB, discul 2 SAN de 100 GB.

### **1.5.4 IBM Cloud Integrated Analytics Large Server**

Un server IBM SoftLayer gestionat de Client, cu specificații minime de 16 nuclee virtuale private, 64 GB RAM, discul 1 SAN de 100 GB, discul 2 SAN de 100 GB.

### **1.5.5 IBM Cloud Integrated Analytics SAN Storage**

Stocarea SAN poate fi adăugată Serverelor ICIA Servers în incremente de 100, 250 sau 500 GB.