

IBM „Cloud Service“ aprašas „IBM Digital Data Exchange“

Toliau pateikiamas jūsų Užsakymo Paslaugos aprašas.

1. „Cloud Service“

„Cloud Service“ pasiūlymas, įskaitant pagrindinį pasiūlymą ir galimas papildomas funkcijas, yra aprašytas toliau, kaip pažymėta Užsakymo dokumente. Užsakymo dokumentą sudarys pateiktas Pasiūlymas ir iš IBM gautas Teisių suteikimo dokumentas (TSD), patvirtinantis „Cloud Services“ pradžios datą, terminą ir sąskaitų teikimo pradžią.

1.1 „IBM Digital Data Exchange“

„IBM Digital Data Exchange“ – tai sprendimas, teikiantis vieną žiniatinklio svetainės konfigūravimo ir visuotinio diegimo sąsają bei puslapių žymas mobiliesiems.

„IBM Digital Data Exchange“ leidžia tvarkyti IBM ir IBM verslo partnerių žymas bei diegti jas jūsų žiniatinklio svetainėje arba svetainėje mobiliesiems. „IBM Digital Data Exchange“ vartotojo sąsaja teikia tiesioginę prieigą prie žymėjimo proceso, todėl vartotojai gali apibrėžti puslapių žymas ir puslapių grupes pagal taisyklių rinkinį ir taip nustatyti žymų vykdymą. Įsigiję „IBM Digital Data Exchange“, galėsite valdyti šiuo metu ir anksčiau keliose aplinkose įdiegtas IBM, IBM verslo partnerių žymas ir pasirinktinį „JavaScript“ arba savo kodą.

2. Saugos aprašas

2.1 Saugos strategijos

IBM palaiko privatumo ir saugos politikas, kurios yra paskelbiamos ir pateikiamos IBM darbuotojams. IBM reikalauja, kad asmenys visame pasaulyje, teikiantys IBM duomenų centrų palaikymą, turėtų privatumo ir saugos mokymus, ir palaiko informacijos apsauga besirūpinančią saugos komandą. IBM saugos strategijos ir standartai kasmet peržiūrimi ir iš naujo įvertinami. IBM saugos incidentai nagrinėjami pagal išsamią reagavimo į incidentus procedūrą.

2.2 Prieigos valdymas

IBM išlaiko loginį kliento duomenų atskyrimą. Išlaikoma kliento duomenų savitoji schema, kurią galima pasiekti naudojantis „Cloud Service“ arba eksportuojant kliento nurodytus duomenis. Prieigą prie „Cloud Service“ ir kliento duomenų kontroliuoja ir valdo priskirtas kliento administratorius. Prieigai prie kliento sistemų IBM naudoja kelių veiksmų autentifikavimą ir šifruoto VPN tunelio technologiją. Prieiga leidžiama tik asmenims, kurie privalo priėti tvarkyti ir administruoti „Cloud Service“ ir susijusią techninės ir programinės įrangos infrastruktūrą trečiosios šalies duomenų centro įrangoje. IBM naudoja WIFI (a/k/a 802.11) tinklo srautą, kuris šifruotas naudojant WPA2 ir AES šifravimo algoritmo parinktį, užtikrina netransliavimo SSID ir abipusį serverio ir galinių įrenginių autentifikavimą prieinančią prie sistemų, kuriose yra kliento duomenys.

2.3 Paslaugos vientisumas ir pasiekiamumas

Operacinės sistemos išteklių (OSI) ir taikomųjų programų programinės įrangos modifikavimus reguliuoja IBM keitimų valdymo procesas. Techninė ir programinė įranga, prieigos žurnalai, tik skaitymo prieiga ir šifravimo valdikliai naudojami tinklo infrastruktūroje ir asmenų, dirbančių IBM duomenų centruose arba su kliento duomenimis IBM duomenų centruose, darbo stotyse, siekiant sumažinti kompiuterinių virusų ir kitų žinomų kenkėjiško kodo formų platinimo ir vykdymo tikimybę. IBM taiko viso tinklo šifravimą standartiniu SSL (https) ryšiu ir IBM infrastruktūroje taikomi technologijos sprendimai, skirti visapusei saugai, įskaitant užkardą, įsilaužimo prevencijos ir apsaugos nuo kenkėjiškų programų technologijas. Duomenų perdavimo valdymo protokolo / interneto protokolo (TCP/IP) pažeidžiamumą periodiškai tikrina įgaliotieji administratoriai, ieškodami potencialių sistemos saugos spragų ir jas šalindami. IBM saugyklos duomenys kopijuojami į antrinę IBM duomenų centro saugyklą, o trečioji šifruota ir dubliuota archyvinė kopija (juosta) saugoma trečiosios šalies atskiroje avarinio atkūrimo įrangoje.

2.4 Veiklos registravimas

IBM pildo savo veiklos sistemose, taikomuosiose programose, duomenų saugyklose, tarpinėje įrangoje ir tinklo infrastruktūros įrenginiuose, kuriuose galima konfigūruoti ir kurie yra konfigūruoti registruoti veiklą, žurnalus. IBM laiko žurnalus, kuriuose įrašomi i) sėkmingi ir nesėkmingi bandymai prisijungti, ii) sėkmingi

ir nesėkmingi bandymai gauti prieigą prie infrastruktūros iš išorinės vietos, iii) prieigos bandymų naujinimais OSR ir iv) veikla, naudojant sistemos arba saugos administratoriaus įgaliojimus.

2.5 Fizinė sauga

IBM ir IBM trečiosios šalies teikiamuose duomenų centruose IBM leidžia prieigą tik IBM duomenų centro įgaliotajam personalui. IBM „Cloud Service“ aplinka apima kelių veiksmų fizinės prieigos autentifikavimą, kurį sudaro unikalūs kodas ir biometrinių duomenų nuskaitymas bei 24 x 7 budintys apsaugos darbuotojai, žmonių užtikrinama apsauga ir stebėjimas vaizdo kameromis. IBM draudžia neteisėtą bet kokios laikmenos, kurioje yra kliento duomenų, peržiūrą, kopijavimą, keitimą arba šalinimą. Keičiamosios laikmenos, kuriose yra kliento duomenys (įskaitant atmintines, kompaktinius ir DVD diskus), šifruojamos naudojant mažiausiai 256 bitų AES (arba atitikmenį). Jei gali būti reikalingos prieigos teisės prie slapto arba kliento duomenų, IBM išduotuose nešiojamuosiuose kompiuteriuose ir skirtose kompiuterizuotose darbo vietose privaloma įdiegti viso disko šifravimą (PGP). Prieš naudodama laikmenas pakartotinai, IBM sunaikina keičiamąsias laikmenas ir visus mobiliuosius įrenginius (pvz., diskus, USB atmintines, DVD, atsarginės kopijos juostas, spausdintuvus ir nešiojamuosius kompiuterius), kuriuose yra kliento duomenų, arba padaro kliento duomenis tokiose fizinėse laikmenose neįskaitomus ir neatkuriamus jokiais techninėmis priemonėmis. Popieriaus atliekas IBM susmulkina ir saugiai bei konfidencialiai sunaikina taip, kad popieriaus atliekos būtų neįskaitomos.

2.6 Atitikimas

IBM kasmet atestuoja privatumo praktikas, kad atitiktų JAV Prekybos departamento „Saugaus uosto“ programos principus dėl pranešimų, pasirinkimo, tolesnio perdavimo, prieigos ir tikslumo, saugos ir priežiūros bei reikalavimų vykdymo. Mūsų gamybos duomenų centruose kasmet atliekamas pramonės standarto SSAE 16 (anksčiau – SAS 70) arba atitinkamo tipo auditas. IBM peržiūri, ar su sauga ir privatumu susijusios veiklos atitinka IBM verslo reikalavimus. Siekdama laikytis informacijos saugos politikų, IBM reguliariai atlieka vertinimus ir auditus. Saugos auditų metu taikomos tinkamos saugos politikos numato periodinį saugos pataisų taikymą ir slaptažodžių valdymą bei kontrolę. Kasmet IBM darbuotojai ir tiekėjai dalyvauja darbuotojų saugos ir žinių apie sukčiavimą mokymo kursuose. Darbuotojams kasmet primenami jų darbo tikslai ir atsakomybė laikytis verslo etikos, konfidencialumo ir IBM saugos įsipareigojimų.

3. Paslaugos lygio tikslai

IBM siekia, kad „IBM SaaS“ būtų pasiekiami Klientui 99 proc. prieinamumo lygiu. PLT nėra sutartinis įsipareigojimas, o veikiau tikslų, kuriuos IBM klientų aptarnavimo komanda stengiasi pasiekti ar viršyti pasinaudodama procedūromis, technologijomis ir žmonėmis, rinkinys.

4. Teisių suteikimo ir sąskaitų išrašymo informacija

4.1 Mokesčio apskaičiavimas

„Cloud Service“ pateikiamas pagal vieną iš šių mokesčių apskaičiavimo metrikų, kaip nurodyta Užsakymo dokumente:

- a. Milijonas serverio iškvietimų (MSC) yra matavimo vienetas, kuriuo remiantis galima gauti „Cloud Service“. Serverio iškvietimas – įvykus pažymėtam įvykiui, kurį inicijavo sekamas lankytojas viename Subjekto ID, „Cloud Service“ perduoti ir inicijuoti duomenys. Serverio iškvietimai, kuriuos apdoroja skirtingi Subjekto ID, bus skaičiuojami kaip unikalūs kiekvieno unikalaus Subjekto ID Serverio iškvietimai. Subjekto ID atskiria ir (arba) valdo prieigos prie „Cloud Service“ duomenų, kurie gali apimti apdorotus duomenis iš vienos ar daugiau jūsų svetainių, teises. Kiekviena MSC teisė yra vienas milijonas Serverio iškvietimų. Reikia įsigyti Milijono serverio iškvietimų teises, pakankamas apdorojamų Serverio iškvietimų skaičiui padengti matavimo laikotarpiu, nurodytu Užsakymo dokumente.

4.2 Mokesčiai ir sąskaitų išrašymas

Mokėtina suma už „Cloud Service“ nurodoma Užsakymo dokumente.

5. Terminas ir atnaujinimo galimybės

5.1 Terminas

„Cloud Service“ naudojimo terminas prasideda nuo dienos, kai IBM praneša jums, kad turite prieigą prie „Cloud Service“, kaip aprašyta Užsakymo dokumente. Užsakymo dokumento TSD skyriuje bus patvirtinta tiksli termino pradžios ir pabaigos data. Termino laikotarpiu jums leidžiama padidinti „Cloud Service“ naudojimo lygį susisiekus su IBM arba IBM verslo partneriu. Didesnį naudojimo lygį patvirtinsime Užsakymo dokumente.

5.2 „Cloud Services“ termino atnaujinimo parinktys

Jūsų Užsakymo dokumente bus apibrėžta, ar laikotarpio pabaigoje „Cloud Service“ naudojimas bus atnaujintas, nurodant vieną iš toliau pateiktų galimybių:

5.2.1 Automatinis atnaujinimas

Jei jūsų Užsakymo dokumente nurodoma, kad atnaujinimas yra automatinis, galite nutraukti besibaigiantį „Cloud Service“ galiojimo terminą pateikę prašymą raštu ne mažiau nei prieš devyniasdešimt (90) dienų iki galiojimo pabaigos datos, nustatytos Užsakymo dokumente. Jei IBM arba jūsų IBM verslo partneris negauna tokio pranešimo apie galiojimo datos nutraukimą, galiojimo terminas bus automatiškai atnaujinamas vieniems metams arba tos pačios trukmės terminui, kaip nustatyta pradiniam TSD.

5.2.2 Nepertraukiamas sąskaitų išrašymas

Kai Užsakymo dokumente nurodoma, kad sąskaitos išrašomos nepertraukiamai, jūs ir toliau turėsite prieigą prie „Cloud Service“ ir už „Cloud Service“ naudojimą jums nepertraukiamai bus išrašomos sąskaitos. Norėdami nutraukti „Cloud Service“ naudojimą ir sustabdyti nepertraukiamo sąskaitų išrašymo procesą, turėsite prieš devyniasdešimt (90) dienų raštu pateikti IBM arba IBM verslo partneriui prašymą atšaukti „Cloud Service“. Atšaukus prieigą, jums bus išrašyta sąskaita už nesumokėtus to mėnesio, kai įsigalios atšaukimas, prieigos mokesčius.

5.2.3 Reikalingas atnaujinimas

Kai Užsakymo dokumente nurodoma, kad atnaujinimo tipas yra „terminuotas“, terminui suėjus „Cloud Service“ teikimas pasibaigs ir jūsų prieiga prie „Cloud Service“ bus pašalinta. Norėdami ir toliau naudoti „Cloud Service“ pasibaigus terminui, turėsite pateikti užsakymą IBM pardavimo atstovui arba IBM verslo partneriui ir įsigyti prenumeratą naujam terminui.

6. Techninis palaikymas

Prenumeratos laikotarpiu, jei taikoma, teikiamas „IBM SaaS“ pasiūlymo ir įgalinimo programinės įrangos techninis palaikymas. Toks techninis palaikymas įtrauktas į „IBM SaaS“ ir kaip atskiras pasiūlymas neteikiamas.

Techninio palaikymo informaciją galima rasti apsilankius http://www-01.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

7. Įgalinimo programinė įranga

- a. „Cloud Service“ pasiūlyme gali būti įgalinimo programinė įranga. Įgalinimo programinę įrangą galite naudoti tik kartu su naudojamu „Cloud Service“ per visą „Cloud Service“ terminą. Jei įgalinimo programinėje įrangoje yra pavyzdinis kodas, papildomai turite teisę kurti išvestinius pavyzdinio kodo darbus ir naudoti juos tik su pagal šią teisę. Įgalinimo programinei įrangai taikoma PSL, jei tokia yra, ir ji teikiama kaip „Cloud Service“ komponentas, tačiau kitu atveju teikiama „TOKIA, KOKIA YRA“.

8. Papildoma informacija

8.1 Teisių suteikimo informacija

Į „IBM Digital Data Exchange“ prenumeratos mokesčių įtraukta:

- a. Jums bus pateiktas vienas „IBM Digital Data Exchange“ egzempliorius.
- b. Standartinis ne daugiau kaip penkių (5) val. nuotoliniu būdu teikiamų įgyvendinimo paslaugų įgalinimas, pirmą kartą diegiant „IBM Digital Data Exchange“. Paslaugų galiojimo laikas baigiasi praėjus 90 dienų nuo dienos, kai IBM įspėja jus, kad prieiga prie „Cloud Service“ teikiama neatsižvelgiant į tai, ar išnaudotos visos valandos.

8.2 Privatumo pranešimas ir politika

Jūs sutinkate (i) pateikti aiškia ir pastebimą nuorodą į savo žiniatinklio svetainės naudojimo sąlygas ir privatumo politiką, kuri apima nuorodą į IBM (<http://www.ibm.com/software/marketing-solutions/privacy/index.html>) ir jūsų duomenų rinkimo ir naudojimo praktikas, (ii) pateikti informaciją, kad IBM veiksda jūsų vardu lankytojo kompiuteryje padeda slapukus ir „clear gifs“ žymas / žiniatinklio indikatorius, ir paaiškinti tokios technologijos tikslą ir naudojimą, taip pat; (iii) kiek reikalauja teisės aktai, prieš padėdami patys arba prieš IBM padedant jūsų vardu žiniatinklio svetainės lankytojo įrenginiuose slapukus ir „clear gifs“ žymas / žiniatinklio indikatorius, gauti žiniatinklio svetainės lankytojų sutikimą.

Jūs žinote ir sutinkate, kad „Cloud Services“ naudojimo ir palaikymo tikslais, naudodama sekimo ir kitas technologijas, IBM gali iš jūsų (jūsų darbuotojų ir rangovų) rinkti su „Cloud Services“ naudojimu susijusią asmens informaciją. IBM renka naudojimo statistinius duomenis ir informaciją apie „Cloud Services“ efektyvumą, kad galėtų gerinti vartotojų patirtį ir (arba) pritaikyti bendravimą su jumis. Jūs patvirtinate, kad

gausite arba jau esate gavę sutikimą leisti IBM apdoroti surinktą asmens informaciją anksčiau nurodytais tikslais, laikantis taikomų įstatymų, IBM, kitose IBM įmonėse ir jų subrangovų vietose, kur IBM ir mūsų subrangovai vykdo veiklą. IBM vykdys jūsų darbuotojų ir rangovų pageidavimus pasiekti, naujinti, taisyti arba panaikinti jų surinktą asmens informaciją.

8.3 Naudos gavimo vietos

Kai taikoma, mokesčiai yra pagrįsti vieta (-omis), kurią (-ias) jūs nurodote kaip gaunančią (-ias) naudą iš „Cloud Services“. IBM taikys mokesčius pagal „Cloud Service“ užsakymo metu nurodytą verslo adresą kaip pagrindinę naudos gavimo vietą, nebent IBM pateiksite papildomos informacijos. Jūs esate atsakingi už tokios informacijos atnaujinimą ir IBM informavimą apie visus pakeitimus.