Politica de confidențialitate Cost Control — web și aplicație mobilă

Versiune: 1.1

Data ultimei actualizări: 30 iulie 2026

1. Pe scurt

Cost Control este o aplicație pentru administrarea utilizatorilor, proiectelor, contractelor, partenerilor de afaceri, facturilor, costurilor, plăților și analizelor financiare. Serviciul este disponibil prin interfața web și aplicația mobilă iOS/Android.

Această politică explică ce date cu caracter personal sunt prelucrate prin Cost Control, de ce, pentru cât timp, cui pot fi divulgate și ce drepturi aveți potrivit Regulamentului (UE) 2016/679 („RGPD”/„GDPR”) și legislației române.

Cost Control este destinat utilizării profesionale de către organizații, nu minorilor și nu consumatorilor în scop personal.

2. Cine este operatorul datelor

2.1 Datele introduse de organizația dumneavoastră

Dacă ați primit contul Cost Control de la angajator, client sau altă organizație („Organizația”), Organizația este operatorul datelor despre utilizatorii săi, persoanele de contact, furnizori, clienți și alte persoane ale căror date sunt introduse în aplicație. Organizația stabilește scopurile și mijloacele prelucrării, accesul utilizatorilor, durata păstrării și configurația instanței.

Cost Control este implementat într-un model de infrastructură controlată de client. Backendul, baza de date și interfața web rulează pe un server, o mașină virtuală sau un cont cloud ales, deținut ori închiriat și administrat de Organizație. Datele operaționale rămân sub controlul administrativ al Organizației și nu sunt transferate automat către Aegis Core Tech doar pentru că Organizația folosește software-ul.

Solicitările privind datele introduse în Cost Control trebuie adresate mai întâi Organizației care v-a furnizat contul. Identitatea și datele sale de contact sunt disponibile în invitația sau documentele contului, în informarea de confidențialitate a angajatorului/clientului ori de la administratorul instanței Cost Control. Această politică de produs completează, dar nu înlocuiește, informarea proprie a Organizației în calitate de operator.

Administratorul platformei desemnat de Organizație gestionează conturile utilizatorilor, inclusiv crearea, dezactivarea și ștergerea acestora. Administratorul sau contactul de confidențialitate al Organizației este și punctul de contact pentru cererile de acces, rectificare și ștergere privind instalarea Cost Control a Organizației.

2.2 Rolul Aegis Core Tech SRL

Furnizorul aplicației este:

Aegis Core Tech SRL
CUI: RO52060129 • Nr. registrul comerțului: J2025046995006
Calea Dorobanți 33A, 010553 București, România
E-mail: contact@aegiscoretech.com
Telefon: +40 741 131 505
Website: https://aegiscoretech.com

Aegis Core Tech furnizează și licențiază software-ul, dar nu găzduiește baza de date de producție și nu are acces permanent sau de rutină la datele operaționale din instanța clientului. Simpla furnizare a licenței, actualizărilor sau documentației, fără acces la date personale, nu face din Aegis Core Tech o persoană împuternicită pentru acele date.

Rolurile sunt următoarele:

- Organizația este operatorul datelor operaționale prelucrate în instanța sa Cost Control;
- Aegis Core Tech este operator distinct pentru propriile date strict necesare contractării, licențierii, facturării, securității relației comerciale și administrării solicitărilor de suport;
- dacă Organizația solicită suport sau mentenanță ce necesită acces la instanță ori la date personale, Aegis Core Tech va acționa, pentru acel acces, ca persoană împuternicită de operator, numai la instrucțiunile documentate ale Organizației, în baza unui contract conform art. 28 RGPD. Accesul trebuie autorizat, limitat în timp, jurnalizat și revocat la finalizarea intervenției;
- furnizorii externi activați sau contractați de Organizație, precum furnizorul său cloud, Microsoft, Google/Firebase, OpenAI ori furnizorul de e-mail, pot primi date conform configurației alese. Aceste transferuri sunt descrise la secțiunile 7 și 8 și nu reprezintă stocare de rutină a bazei de date de producție de către Aegis Core Tech.

Faptul că infrastructura este controlată de Organizație nu limitează obligațiile Aegis Core Tech privind securitatea produsului și protecția datelor prin proiectare. Organizația comunică utilizatorilor identitatea și datele sale de contact prin aplicație, invitația de cont, contract sau propria informare de confidențialitate.

3. Ce date prelucrăm

În funcție de funcțiile folosite și de configurația stabilită de Organizație, pot fi prelucrate următoarele categorii:

3.1 Cont, autentificare și autorizare

- identificator intern de utilizator, nume de utilizator, prenume și nume dacă sunt configurate de backend, adresă profesională de e-mail;
- roluri, permisiuni, apartenența la proiecte și starea contului;
- credențiale protejate criptografic; parola în clar nu trebuie păstrată;
- tokenuri de sesiune, data/ora conectării, evenimente de autentificare și deconectare;
- pentru autentificarea Microsoft Entra ID: identificatori și atribute de cont furnizate de Microsoft conform configurației tenantului, precum numele, adresa de e-mail și identificatorul contului;
- motivul dezactivării unui cont, introdus de un administrator.

3.2 Date profesionale, contractuale și financiare

- date despre proiecte și membri de proiect;

- denumiri și identificatori fiscali ai partenerilor de afaceri; aceștia devin date personale dacă identifică o persoană fizică, PFA sau reprezentant;
- numele, e-mailul și numărul de telefon ale persoanelor de contact;
- contracte: număr, perioadă, valoare, condiții de plată, garanții, note și linkul/documentul asociat;
- facturi și poziții de factură: număr, dată, scadență, descriere, valori, partener, stare și istoric;
- plăți: sume, date, metodă, referință de tranzacție și descriere;
- costuri, categorii, alocări pe proiect, venituri, cheltuieli și indicatori/previziuni financiare;
- marcaje temporale de creare și modificare și, dacă backendul este configurat astfel, identitatea utilizatorului care a efectuat operațiunea.

Organizația trebuie să evite introducerea datelor care nu sunt necesare scopului profesional și să informeze persoanele de contact ale căror date sunt introduse indirect, conform art. 14 RGPD.

3.3 Asistentul AI și mesajele vocale

Funcția AI este inactivă dacă administratorul Organizației nu o configurează și nu furnizează credențialele necesare ale furnizorilor. Atunci când este activată, funcția poate prelucra:

- întrebările, textul mesajelor, un identificator al conversației și răspunsurile generate prin serviciul de chat OpenAI;
- fișierul audio înregistrat la cererea utilizatorului și trimis serviciului de transcriere OpenAI;
- textul transmis serviciului text-to-speech OpenAI pentru generarea răspunsului audio;
- informațiile extrase prin instrumente autorizate din baza de date Cost Control a Organizației, când sunt necesare pentru a răspunde cererii, cu respectarea rolurilor și permisiunilor existente ale utilizatorului;
- cuvinte-cheie de căutare filtrate, trimise către Tavily atunci când asistentul are nevoie de o căutare web actuală, împreună cu metadatele tehnice ale cererii prelucrate de furnizor.

Aplicația este proiectată să elimine informațiile confidențiale din termenii de căutare Tavily înainte de transmitere. Un termen de căutare poate constitui totuși dată personală dacă privește sau identifică o persoană. Utilizatorii nu trebuie să solicite asistentului divulgarea secretelor, datelor din categorii speciale, parolelor sau altor informații care nu sunt necesare operațiunii cerute.

Înregistrarea microfonului începe numai după o acțiune a utilizatorului și după permisiunea acordată prin sistemul de operare. Permisiunea poate fi retrasă din setările dispozitivului.

Cost Control nu păstrează conversațiile AI ca istoric în backend. Mesajele sunt ținute în memoria aplicației mobile numai cât timp chatul este activ și sunt eliminate când acesta este închis sau părăsit. Backendul prelucrează tranzitoriu prompturile, rezultatele relevante ale instrumentelor, fișierele audio, transcrierile și răspunsurile pentru finalizarea cererii. OpenAI și Tavily prelucrează datele conform contului, configurației API, contractului și controalelor de date alese de Organizație, astfel cum este explicat la secțiunile 7–9.

3.4 Aplicația mobilă și notificările push

- token Firebase Cloud Messaging („FCM”) și Firebase Installation ID;
- platforma (Android/iOS), versiunea aplicației, metadate Firebase/dispozitiv, identificatorul buildului sistemului de operare Android (`Build.ID`) sau Identifier for Vendor („IDFV”) pe iOS;
- titlul, conținutul tehnic și ruta internă („deep link”) a notificării;

- pe dispozitiv: tokenul de autentificare, profilul utilizatorului, limba aleasă, URL-urile backend salvate și cache-ul unităților de măsură;
- temporar, fișierul audio creat pentru trimiterea unui mesaj vocal.

Notificările sunt opționale la nivelul sistemului de operare. Refuzul lor nu trebuie să împiedice folosirea funcțiilor de bază ale aplicației. Evităm includerea datelor financiare sau personale sensibile în textul afișat pe ecranul blocat.

3.5 Date tehnice și de securitate

Serverul și infrastructura pot prelucra adresa IP, data și ora cererii, URL-ul/endpointul, tipul dispozitivului, browserul și sistemul de operare, codul de răspuns, identificatori de sesiune, evenimente de securitate și erori tehnice. Aceste date sunt folosite pentru operare, diagnosticare, prevenirea abuzului și securitate.

Conținutul și retenția logurilor sunt stabilite de Organizația care administrează infrastructura, cu respectarea minimizării datelor și a limitării stocării. Organizația trebuie să vă informeze separat dacă activează un serviciu extern de monitorizare sau raportare a erorilor.

4. De unde provin datele

Datele pot proveni:

- direct de la utilizator;
- de la Organizație și administratorii săi;
- de la alți utilizatori autorizați care introduc date de contact sau documente comerciale;
- de la Microsoft, când este folosită autentificarea Entra ID;
- de la dispozitiv, sistemul de operare și Firebase pentru notificări;
- de la OpenAI, când asistentul AI returnează text, transcrieri sau voce generată;
- de la Tavily și surse web publice, când asistentul AI efectuează o căutare web;
- din sisteme financiar-contabile importate sau integrate de Organizație. Organizația este responsabilă să informeze persoanele despre integrările pe care le activează.

Dacă datele nu au fost obținute direct de la persoana vizată, operatorul trebuie să furnizeze informarea prevăzută de art. 14 RGPD, cu excepțiile strict prevăzute de lege.

5. Scopuri și temeiuri juridice

Scop	Categorii principale	Temei juridic uzual
Crearea și administrarea contului, autentificare, roluri și sesiuni	cont, profil, roluri, tokenuri	art. 6 alin. (1) lit. b RGPD pentru contractul cu utilizatorul individual, unde este cazul; de regulă art. 6 alin. (1) lit. f pentru operarea serviciului B2B și securitate; pentru angajați, temeiul este stabilit de angajator
Gestionarea proiectelor, contractelor, facturilor, costurilor și plăților	date profesionale și financiar-contabile	art. 6 alin. (1) lit. b, c și/sau f RGPD, în funcție de relația cu persoana și obligațiile contabile/fiscale
Evidență contabilă și răspuns la autorități	documente justificative și operațiuni financiare	art. 6 alin. (1) lit. c RGPD, inclusiv Legea contabilității nr. 82/1991 și legislația fiscală aplicabilă
Securitate, prevenirea fraudei, audit și apărarea drepturilor	loguri, IP, evenimente, marcaje temporale	art. 6 alin. (1) lit. f RGPD; art. 6 alin. (1) lit. c când există o obligație legală
Autentificare Microsoft Entra ID	identificatori și atribute de cont	art. 6 alin. (1) lit. b sau f RGPD, în funcție de relație și configurația Organizației
Asistent AI text/voce și căutare web AI	prompturi, rezultate autorizate din baza de date, audio, transcrieri, răspunsuri și termeni de căutare filtrați	art. 6 alin. (1) lit. b sau f pentru funcția solicitată; accesul la microfon și informarea vizibilă necesară sunt controlate separat în fluxul mobil. Consimțământul nu va fi invocat ca temei RGPD decât dacă fluxul implementat permite un consimțământ liber și retragerea lui fără consecințe nejustificate
Notificări push	token FCM, identificator dispozitiv, platformă, versiune	art. 6 alin. (1) lit. f sau b pentru comunicări operaționale solicitate; permisiunea dispozitivului este separată. Comunicările promoționale, dacă vor exista, necesită un temei și mecanism de opt-out distinct
Suport tehnic	date de contact, conținutul cererii, loguri furnizate	art. 6 alin. (1) lit. b și/sau f RGPD

Interesul legitim este folosit numai după verificarea necesității și a balanței cu drepturile persoanei. Puteți solicita informații despre evaluarea interesului legitim și vă puteți opune în condițiile art. 21 RGPD.

Nu condiționăm funcțiile de bază de consimțământ pentru prelucrări care nu sunt necesare. Atunci când prelucrarea se bazează pe consimțământ, acesta poate fi retras oricând, fără a afecta legalitatea prelucrării anterioare.

6. Date speciale și identificatori naționali

Cost Control nu este proiectat să solicite date privind sănătatea, originea rasială sau etnică, opiniile politice, convingerile religioase, apartenența sindicală, viața sexuală, orientarea sexuală, date genetice ori biometrice folosite pentru identificare. Vocea este prelucrată ca înregistrare audio, nu pentru identificare biometrică.

Nu introduceți asemenea informații în câmpurile libere, documente sau conversații AI. Dacă Organizația decide că sunt strict necesare, aceasta trebuie să identifice o condiție din art. 9 RGPD, să documenteze necesitatea și să aplice măsuri suplimentare.

Codul numeric personal, seria/numărul actului de identitate și alți identificatori naționali nu trebuie introduși decât dacă sunt necesari și există un temei din art. 6 RGPD. Dacă se invocă interesul legitim, se aplică garanțiile speciale din art. 4 al Legii nr. 190/2018: minimizare, securitate/confidențialitate, termene de păstrare/ștergere și instruirea periodică a personalului.

7. Cui divulgăm datele

Accesul este limitat la utilizatorii autorizați ai Organizației, conform rolurilor și permisiunilor, și la personalul/furnizorii care au nevoie legitimă de acces.

În funcție de configurație, destinatarii sau persoanele împuternicite pot include:

Furnizor/categorie	Rol și date	Observații
Infrastructura controlată de Organizație și, dacă este cazul, furnizorul cloud contractat de aceasta	găzduirea bazei de date, API și web	Organizația deține, închiriază sau administrează mediul și comunică utilizatorilor furnizorul și țara/regiunea aplicabilă
Google Firebase Cloud Messaging	livrare notificări; token FCM, identificatori tehnici, metadate mesaj/dispozitiv	Activ în aplicația mobilă; politica Google/Firebase se aplică serviciului furnizat
Microsoft Entra ID	autentificare opțională; identificatori și atribute de cont	Numai dacă Organizația activează conectarea Microsoft
OpenAI	răspunsuri de chat, transcriere vocală și text-to-speech; prompturi, date relevante returnate de instrumentele Cost Control autorizate, audio, transcrieri și răspunsuri	Numai dacă Organizația activează AI și gestionează cheia API OpenAI, contractul, proiectul, controalele de date și regiunea de procesare disponibilă. OpenAI declară că datele API nu sunt folosite implicit pentru antrenarea modelelor, în lipsa opțiunii exprese a clientului. Se aplică controalele de date API și politica de confidențialitate OpenAI
Tavily	căutare web actuală pentru asistentul AI; cuvinte-cheie filtrate și metadate tehnice ale cererii	Numai dacă Organizația activează instrumentul de căutare web AI și gestionează cheia API și contractul Tavily. Cost Control este proiectat să excludă informațiile confidențiale din termenii de căutare înainte de transmitere. Prelucrarea este guvernată de politica de confidențialitate Tavily și condițiile comerciale aplicabile
Furnizorul de e-mail ales de Organizație	mesaje de sistem și resetarea parolei; Aegis poate folosi propriul furnizor pentru răspunsurile de suport adresate direct Aegis	Furnizorul concret depinde de configurația Organizației
Consultanți, auditori, autorități și instanțe	conformitate, audit, apărarea drepturilor și obligații legale	numai când există o necesitate și un temei legal

Nu vindem date personale. Nu folosim datele operaționale ale Organizației pentru publicitate comportamentală.

Operatorul trebuie să mențină lista actuală a persoanelor împuternicite/subîmputernicite și, unde este aplicabil, să informeze Organizația despre modificări conform contractului art. 28 RGPD.

8. Transferuri internaționale

Instalarea Cost Control este găzduită pe infrastructura aleasă și controlată de Organizație. Organizația comunică utilizatorilor țara/regiunea de găzduire și este responsabilă să se asigure că alegerea respectă RGPD. Informația aplicabilă instalării dumneavoastră poate fi obținută de la administratorul acesteia. Folosirea Microsoft, Google/Firebase, OpenAI, Tavily sau a altor furnizori poate implica acces ori transfer de date în afara Spațiului Economic European.

Localizarea Organizației sau crearea contului furnizorului din Uniunea Europeană nu garantează, în sine, că întreaga procesare API are loc în UE. Regiunea efectivă depinde de disponibilitatea serviciului, endpointul API, configurația contului/proiectului și contractul ales de Organizație. Administratorul trebuie să documenteze aceste setări înaintea activării furnizorului.

Un astfel de transfer va avea loc numai în baza unui mecanism permis de capitolul V RGPD, cum ar fi:

- o decizie de adecvare a Comisiei Europene, inclusiv Cadrul UE–SUA privind confidențialitatea datelor pentru entitățile certificate și categoriile acoperite;
- clauzele contractuale standard ale Comisiei Europene, împreună cu evaluarea impactului transferului și măsuri suplimentare, dacă sunt necesare;
- o altă derogare sau garanție legală aplicabilă.

Puteți solicita informații despre mecanismul folosit și o copie a garanțiilor, cu eliminarea informațiilor confidențiale.

9. Cât timp păstrăm datele

Operatorul stabilește o politică documentată de retenție. În lipsa unei obligații mai lungi, datele se șterg sau se anonimizează când nu mai sunt necesare.

Categorie	Perioadă sau criteriu de păstrare
Cont și profil	până când un administrator șterge contul și pentru orice perioadă suplimentară impusă de obligații legale sau apărarea drepturilor. Cost Control nu șterge automat un cont după o perioadă de inactivitate
Token de sesiune pe dispozitiv	până la deconectare, revocare, expirare sau ștergerea aplicației/datelor locale
Token FCM și identificatori ai dispozitivului	înregistrarea dispozitivului curent este eliminată la deconectare, iar înregistrările din backend sunt șterse la ștergerea contului sau când le elimină administratorul. În prezent nu există un mecanism automat de expirare pentru celelalte tokenuri FCM inactive ori invalide, astfel încât acestea pot rămâne până la ștergerea contului sau curățarea manuală de către administrator
Înregistrare audio temporară pe dispozitiv	stocată în directorul temporar al aplicației din sistemul de operare pe durata înregistrării și transmiterii. Nu este adăugată istoricului conversației Cost Control. Fișierul temporar poate rămâne până când este suprascris de o înregistrare ulterioară, eliminat de sistemul de operare sau șters odată cu datele locale ale aplicației
Conversația AI în Cost Control	păstrată în memoria aplicației mobile numai cât timp chatul este activ și eliminată când acesta este închis sau părăsit; backendul Cost Control nu salvează istoricul conversației
Date prelucrate prin OpenAI	conform endpointului API și controalelor alese de Organizație. În configurația API standard OpenAI, conținutul clientului poate fi inclus în loguri de monitorizare a abuzului păstrate până la 30 de zile, dacă nu se aplică un alt control aprobat sau o obligație legală. Unele endpointuri au perioade distincte pentru starea aplicației; administratorul trebuie să documenteze endpointurile și controalele activate
Căutări web Tavily	conform contractului și configurației Tavily ale Organizației. Politica generală Tavily arată că datele interogărilor sunt păstrate cât este necesar serviciului și că anumite părți pot fi folosite pentru îmbunătățirea răspunsurilor dacă acordul cu clientul nu prevede altfel. Organizația trebuie să verifice termenii de retenție ai planului folosit
Loguri tehnice și de securitate	pe perioada necesară operării, securității și investigării incidentelor; logurile asociate unei investigații pot fi păstrate până la finalizarea acesteia și a eventualelor demersuri legale
Documente financiar-contabile care intră sub Legea nr. 82/1991	5 ani calculați de la 1 iulie a anului următor încheierii exercițiului financiar în care au fost întocmite, conform art. 23 și 25, dacă nu se aplică o normă specială mai lungă
Contracte și dovezi necesare apărării drepturilor	pe durata contractului și a termenelor legale aplicabile; termenul general de prescripție este, de regulă, 3 ani conform art. 2517 Cod civil, dar pot exista termene speciale
Backupuri	până la expirarea ciclului de rotație configurat pentru instalarea concretă a clientului. Ciclul exact poate fi obținut prin e-mail de la administratorul sau contactul de confidențialitate al Organizației. Datele șterse nu sunt restaurate în sistemul activ decât dacă restaurarea este necesară pentru continuitate sau obligații legale

Ștergerea din sistemul activ poate să nu elimine imediat datele din backupurile izolate. Acestea trebuie să expire prin rotație și să nu fie reutilizate în alte scopuri.

10. Cookie-uri, stocare web și stocare mobilă

10.1 Interfața web

Cookie-urile ori tehnologiile similare strict necesare autentificării, securității, echilibrării încărcării sau păstrării preferințelor pot fi folosite fără consimțământ numai în limitele excepției legale aplicabile. Orice cookie sau identificator opțional de analiză, personalizare ori marketing trebuie blocat până la consimțământul informat, specific și retragibil, conform art. 5 alin. (3) din Directiva 2002/58/CE și art. 4 alin. (5) din Legea nr. 506/2004.

Organizația care administrează instanța este responsabilă pentru inventarul cookie-urilor și tehnologiilor similare din mediul său. Dacă Organizația adaugă tehnologii opționale de analiză, personalizare sau marketing, aceasta trebuie să ofere înainte de activare opțiuni echivalente „Acceptă”, „Refuză” și setări granulare și să publice numele, furnizorul, scopul și durata fiecărei tehnologii.

10.2 Aplicația mobilă

Aplicația stochează local datele descrise la secțiunea 3.4 pentru sesiune, configurare și funcționare. Permisiunile pentru notificări și microfon sunt administrate prin iOS/Android. Ștergerea aplicației elimină, în mod normal, datele sale locale, dar nu șterge automat datele de pe server; pentru acestea trebuie folosită procedura de ștergere a contului de la secțiunea 13.1.

11. Securitate

Aplicăm sau solicităm, proporțional cu riscul, măsuri precum:

- control al accesului pe roluri și permisiuni și principiul accesului minim;
- autentificare, expirarea/revocarea sesiunilor și dezactivarea conturilor;
- criptarea comunicațiilor prin TLS în producție;
- protejarea credențialelor și secretelor, jurnalizare de securitate și monitorizare;
- copii de siguranță, restaurare testată, actualizări și gestionarea vulnerabilităților;
- acorduri de confidențialitate, instruire și contracte art. 28 RGPD;
- procese de răspuns la incidente și evaluări periodice.

Niciun sistem nu poate garanta securitate absolută. Dacă o încălcare a securității datelor este probabil să genereze un risc, operatorul notifică autoritatea competentă fără întârzieri nejustificate și, dacă este posibil, în cel mult 72 de ore de la luarea la cunoștință (art. 33 RGPD). Persoanele afectate sunt informate când este probabil un risc ridicat (art. 34 RGPD).

Aplicația mobilă se conectează la adresa backend configurată pentru instalarea respectivă. Organizația trebuie să furnizeze și să configureze un endpoint HTTPS/TLS în producție. Un endpoint HTTP necriptat trebuie folosit numai într-un mediu izolat de dezvoltare, deoarece datele trimise către acesta nu ar fi protejate în tranzit.

12. AI, previziuni și decizii automatizate

Cost Control poate genera răspunsuri AI și previziuni/indicatori financiari. Rezultatele pot fi inexacte și trebuie verificate de o persoană competentă. Sistemul nu este destinat să ia, fără intervenție umană, decizii care produc efecte juridice sau afectează în mod similar și semnificativ o persoană.

Dacă Organizația configurează ulterior o asemenea utilizare, trebuie să efectueze înainte o analiză juridică și, după caz, o evaluare a impactului (DPIA), să ofere informații despre logica implicată și consecințe și să asigure dreptul la intervenție umană, exprimarea punctului de vedere și contestarea deciziei, conform art. 22 și 35 RGPD.

13. Drepturile dumneavoastră

În condițiile RGPD, aveți dreptul:

- să fiți informat(ă) (art. 12–14);
- să obțineți acces la date și o copie (art. 15);
- la rectificarea datelor inexacte (art. 16);
- la ștergere, când sunt îndeplinite condițiile legale (art. 17);
- la restricționarea prelucrării (art. 18);
- la portabilitatea datelor furnizate, când se aplică (art. 20);
- să vă opuneți prelucrării bazate pe interes legitim (art. 21);
- să nu faceți obiectul unei decizii exclusiv automatizate în condițiile art. 22;
- să vă retrageți consimțământul, dacă acesta este temeiul prelucrării, fără a afecta prelucrarea anterioară (art. 7 alin. 3);
- să depuneți o plângere și să vă adresați instanțelor.

Trimiteți cererea operatorului indicat la secțiunea 2. Dacă Aegis Core Tech este doar persoană împuternicită, va transmite cererea Organizației sau o va sprijini să răspundă. Putem solicita informații rezonabile pentru verificarea identității, fără a colecta excesiv date.

Operatorul răspunde fără întârzieri nejustificate și, de regulă, în cel mult o lună. Termenul poate fi prelungit cu încă două luni pentru cereri complexe sau numeroase, cu informarea persoanei în prima lună. Cererile sunt, de regulă, gratuite; se aplică excepțiile art. 12 alin. (5) RGPD.

Ștergerea poate fi refuzată sau limitată atunci când păstrarea este necesară pentru o obligație legală, inclusiv contabilă/fiscală, ori pentru constatarea, exercitarea sau apărarea unui drept în instanță. În aceste situații, datele vor fi restricționate la scopurile permise.

13.1 Procedura de ștergere a contului

Conturile Cost Control sunt create și administrate de administratorul platformei desemnat de Organizație; aplicația nu oferă ștergerea autonomă a contului. Pentru a solicita ștergerea, trimiteți un e-mail administratorului sau contactului de confidențialitate al Organizației, folosind adresa comunicată în invitația de cont, contract, informarea de confidențialitate a Organizației ori informațiile de contact afișate pentru instalarea Cost Control respectivă. Organizația trebuie să pună acest canal exact de contact la dispoziția utilizatorilor într-un loc ușor accesibil.

Organizația verifică identitatea solicitantului și soluționează cererea în calitate de operator. Aceasta răspunde fără întârzieri nejustificate și, de regulă, în cel mult o lună. Dacă ștergerea este aprobată,

administratorul șterge profilul activ fără întârzieri nejustificate și, în mod normal, în cel mult 30 de zile de la verificare, dacă nu se aplică o excepție legală.

Ștergerea contului include profilul și setările utilizatorului, numele, adresa de e-mail, informațiile de autentificare și conectare, rolurile și permisiunile, precum și înregistrările dispozitivelor pentru notificări push și tokenurile FCM asociate contului din backend. Sesiunile trebuie revocate. Referințele din jurnalele de audit pot fi anonimizate sau păstrate dacă sunt necesare pentru securitate, responsabilitate, obligații legale ori apărarea drepturilor.

Ștergerea contului nu elimină automat facturile, contractele, plățile, înregistrările de proiect sau alte evidențe comerciale care aparțin Organizației ori privesc alte persoane. Identificatorii personali din aceste evidențe trebuie șterși, anonimizați, restricționați sau păstrați de Organizație potrivit temeiului legal și obligațiilor sale de retenție. Copiile reziduale din backupuri izolate expiră conform ciclului de rotație specific instalării, descris la secțiunea 9.

Nu există un mecanism automat de ștergere a contului exclusiv în baza unei perioade de inactivitate.

14. Plângeri la autoritatea de supraveghere

Vă încurajăm să contactați mai întâi operatorul. De asemenea, puteți depune o plângere la autoritatea din statul membru în care locuiți, lucrați sau considerați că a avut loc încălcarea.

În România:

Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)
B-dul G-ral Gheorghe Magheru nr. 28–30, Sector 1, 010336 București
Website: https://www.dataprotection.ro/
Pagina de plângeri: https://www.dataprotection.ro/?page=Plangeri_pagina_principala

15. Date obligatorii și consecințele nefurnizării

Câmpurile marcate obligatoriu sunt necesare pentru cont sau pentru operațiunea comercială aleasă. Dacă nu furnizați datele de autentificare, nu putem deschide sesiunea. Dacă nu furnizați câmpurile obligatorii ale unei facturi, plăți, relații contractuale sau configurații, acea funcție nu poate fi finalizată. Microfonul, notificările și autentificarea Microsoft sunt opționale dacă rămân disponibile metode alternative.

16. Minori

Serviciul este B2B și destinat persoanelor autorizate de o organizație. Nu este oferit direct copiilor și nu urmărim colectarea intenționată a datelor minorilor. Dacă aflați că astfel de date au fost introduse fără temei, contactați operatorul.

17. Modificarea politicii

Putem actualiza politica pentru schimbări juridice, tehnice sau operaționale. Versiunea curentă, data și un rezumat al modificărilor vor fi disponibile în aplicație și/sau pe pagina publică. Pentru schimbări materiale, utilizatorii vor fi informați printr-un canal adecvat înainte ca acestea să producă efecte, când legea impune.

18. Contact

Pentru datele controlate de Organizație, contactați administratorul instanței Cost Control sau folosiți datele din invitația de cont, contractul ori informarea de confidențialitate furnizată de Organizație.

Pentru prelucrările proprii Aegis Core Tech sau întrebări despre furnizor:

- E-mail: contact@aegiscoretech.com
- Adresă: Calea Dorobanți 33A, 010553 București, România
- Telefon: +40 741 131 505