

# Acord de prelucrare a datelor (DPA)

Ultima actualizare: 1 mai 2026 · Contract conform art. 28 din GDPR.

Aceasta este o traducere oferită doar cu titlu informativ. Dacă există diferențe între această traducere și versiunea în engleză, prevalează versiunea în engleză.

## Cum funcționează

Prezentul DPA face parte din condițiile de utilizare. Se aplică automat atunci când este creat un spațiu de lucru și în el sunt salvate date cu caracter personal. Organizația clientului care deține spațiul de lucru este operatorul; Dazr este persoana împuternicită de operator. Nu este necesară o semnătură; dacă procesul dumneavoastră de achiziții cere un exemplar semnat de ambele părți, scrieți la [legal@dazr.eu](mailto:legal@dazr.eu).

## 1. Definiții

Termenii din prezentul DPA au înțelesul dat de Regulamentul (UE) 2016/679 (GDPR). „Datele personale ale clientului” sunt datele cu caracter personal pe care operatorul (sau membrii și auditorii care acționează sub autoritatea sa) le introduce în spațiul de lucru, inclusiv datele cu caracter personal din sarcinile de control, dovezi, comentarii, fișiere, riscuri, incidente, fișele furnizorilor, membri și invitații, sesizările primite prin portalul public și jurnalul de activitate.

## 2. Obiect, durată, natură și scop

- Obiect: prelucrarea datelor personale ale clientului, astfel încât operatorul să își poată gestiona programul de conformitate privind securitatea informațiilor și protecția datelor prin platforma Dazr Compliance.
- Durată: durata abonamentului operatorului, plus perioada de grație de după încetare prevăzută în condițiile de utilizare.
- Natură și scop: găzduire, stocare, transmitere, consultare, ștergere și operațiunile descrise în condițiile de utilizare și în politica de confidențialitate.
- Tipul de date cu caracter personal: date de identificare ale membrilor spațiilor de lucru și ale auditorilor invitați (e-mail, nume, rol); după caz, date de identificare ale persoanelor care fac sesizări prin portalul public și ale celor care raportează incidente; date de contact ale angajatorilor și metadate operaționale încărcate de operator. Operatorul se asigură că nu încarcă categorii speciale de date decât dacă propriul temei juridic permite acest lucru.
- Categoriile de persoane vizate: angajații, colaboratorii și auditorii externi invitați ai operatorului, precum și orice persoană identificată în conținutul de conformitate pe care operatorul decide să îl încarce.

## 3. Obligațiile persoanei împuternicite

1. Prelucrăm datele personale ale clientului numai pe baza instrucțiunilor documentate ale operatorului. Instrucțiunile constau în utilizarea funcțiilor prevăzute ale platformei; dacă apreciem că o instrucțiune încalcă GDPR sau alte dispoziții privind protecția datelor din dreptul Uniunii sau al unui stat membru, informăm operatorul.
2. Ne asigurăm că persoanele autorizate să prelucreze datele personale ale clientului s-au angajat să respecte confidențialitatea.
3. Luăm toate măsurile impuse de art. 32 din GDPR (securitatea prelucrării). Măsurile actuale sunt descrise în secțiunea 7.
4. Respectăm condițiile de la art. 28 alin. (2) și (4) privind recurgerea la alte persoane împuternicite (a se vedea secțiunea 6).
5. Ținând seama de natura prelucrării și de informațiile de care dispunem, sprijinim operatorul în răspunsul la cererile persoanelor vizate, în notificarea încălcărilor, în evaluările impactului și în consultarea prealabilă a

autorităților de supraveghere [art. 28 alin. (3) lit. (e) și (f)].

6. La alegerea operatorului, la încheierea prestării serviciilor ștergem sau returnăm toate datele personale ale clientului și ștergem copiile existente, cu excepția cazului în care dreptul Uniunii sau al unui stat membru impune stocarea lor.
7. Punem la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea art. 28 și permitem și contribuim la audituri, inclusiv inspecții (a se vedea secțiunea 9).

## 4. Obligațiile operatorului

---

- Operatorul garantează că are un temei juridic conform art. 6 (și, după caz, art. 9) pentru datele cu caracter personal pe care le introduce în spațiul de lucru.
- Operatorul răspunde de exactitatea datelor personale ale clientului și de răspunsul la cererile persoanelor vizate privind spațiul său de lucru (îi transmitem cererile pe care le primim și îl sprijinim conform art. 28 alin. (3) lit. (e)).
- Operatorul controlează accesul (rolurile membrilor, invitațiile auditorilor, portalul public de sesizări) prin setările platformei.

## 5. Transferuri internaționale

---

În mod implicit, datele personale ale clientului sunt stocate în Uniunea Europeană. Atunci când o altă persoană împuternicită are sediul în afara UE, transferurile sunt reglementate de clauzele contractuale standard ale Comisiei Europene (Decizia 2021/914), modulul 3 (de la persoană împuternicită la persoană împuternicită), cu măsurile suplimentare descrise în secțiunea 7. Lista actuală a celorlalte persoane împuternicite și locațiile lor se află la /legal/subprocessors.

## 6. Alte persoane împuternicite (subprocesatori)

---

1. Operatorul ne autorizează să recurgem la alte persoane împuternicite pentru furnizarea serviciului. Lista actuală se află la /legal/subprocessors.
2. Informăm operatorul despre orice adăugare sau înlocuire planificată cu cel puțin 30 de zile înainte, prin abonamentul prin e-mail de pe acea pagină sau prin e-mail către proprietarul spațiului de lucru.
3. Operatorul se poate opune pentru motive rezonabile legate de protecția datelor. Dacă nu putem da curs obiecției, operatorul poate rezilia serviciul afectat și primește o rambursare proporțională pentru partea neutilizată din perioada de facturare în curs.
4. Impunem prin contract scris fiecărei alte persoane împuternicite obligații de protecție a datelor cel puțin la fel de protectoare ca cele din prezentul DPA și rămânem răspunzători față de operator pentru îndeplinirea obligațiilor acesteia.

## 7. Măsuri de securitate (art. 32)

---

- Criptare. Datele personale ale clientului sunt criptate în repaus cu AES-256-GCM la nivelul aplicației, pe lângă criptarea furnizorului de stocare. Întregul transport are loc prin HTTPS cu HSTS preîncărcat, fără variantă necriptată. Cheile sunt derivate prin HKDF dintr-un secret principal păstrat numai în variabilele de mediu ale infrastructurii de producție.
- Controlul accesului. Control al accesului bazat pe roluri în platformă (proprietar, administrator, membru, auditor); sesiuni de auditor limitate în timp și revocabile. Accesul operațional este limitat la o echipă mică de asistență, prin portalul de asistență, care prin concepție afișează doar metadate.
- Autentificare. Autentificare fără parolă, cu cod de unică folosință. Tokenuri de sesiune semnate HMAC, cu valabilitate limitată. Limitarea numărului de cereri la fiecare punct de acces public, inclusiv la autentificarea de administrare.
- Reziliență și integritate. Jurnal de activitate în care se poate doar adăuga, pentru fiecare acțiune care modifică

o stare. Copii de rezervă în UE. Integritatea datelor stocate este verificată prin etichete de autentificare AEAD; un text criptat modificat generează o eroare și nu este livrat.

- Rețea și antete. Content-Security-Policy strictă, cu o listă de scripturi inline permise prin hash, X-Frame-Options strict, X-Content-Type-Options nosniff și HSTS preîncărcat.
- Gestionarea vulnerabilităților. Dependențele au versiuni fixate; urmărim avertizările de securitate și aplicăm corecții într-un termen adecvat gravității.

## 8. Încălcarea securității datelor cu caracter personal

---

Dacă aflăm de o încălcare a securității care afectează datele personale ale clientului, îl notificăm pe proprietarul spațiului de lucru fără întârzieri nejustificate și cel târziu în 72 de ore de la momentul în care am luat cunoștință de aceasta [art. 33 alin. (2)]. Notificarea descrie, în măsura în care sunt cunoscute: natura încălcării, consecințele probabile, măsurile luate sau propuse și punctul de contact pentru informații suplimentare. Sprijinim operatorul în îndeplinirea propriilor obligații de notificare prevăzute la art. 33 și 34.

## 9. Audituri

---

Operatorul (sau un auditor terț mandatat de acesta) poate verifica respectarea prezentului DPA o dată la douăsprezece luni, cu o notificare scrisă de cel puțin 30 de zile și în timpul programului de lucru, astfel încât să nu ne perturbe în mod nerezonabil activitatea și să respecte confidențialitatea datelor altor clienți. Putem percepe o taxă rezonabilă pentru auditurile care depășesc această limită. Atunci când o obligație de audit prevăzută la art. 28 alin. (3) lit. (h) poate fi îndeplinită printr-o atestare a unui terț pe care o deținem, o furnizăm în locul unui audit la fața locului.

## 10. Răspundere

---

Răspunderea fiecărei părți în temeiul prezentului DPA este supusă limitelor din condițiile de utilizare. Aceste limite nu restrâng răspunderea pentru prejudiciile suferite de persoanele vizate în temeiul art. 82 din GDPR.

## 11. Durată și încetare

---

Prezentul DPA se aplică atât timp cât prelucrăm date personale ale clientului și rămâne în vigoare după încetarea condițiilor de utilizare în măsura și pe durata în care încă deținem astfel de date. Secțiunile 8 (încălcări), 9 (audituri) și 12 (returnare și ștergere) rămân în vigoare după încetare.

## 12. Returnare și ștergere

---

La încetarea serviciului, operatorul poate exporta datele spațiului de lucru cu instrumentele de export ale platformei în perioada de grație de 30 de zile prevăzută în condițiile de utilizare. După această perioadă ștergem datele personale ale clientului; copiile de rezervă expiră conform calendarului nostru de păstrare. Datele pe care suntem obligați să le păstrăm (de exemplu, facturile conform dreptului comercial italian) sunt păstrate numai pe durata acestei obligații.

## 13. Ordinea de prioritate

---

În caz de conflict între prezentul DPA și condițiile de utilizare sau politica de confidențialitate, prezentul DPA prevalează în ceea ce privește prelucrarea datelor. Clauzele contractuale standard încorporate pentru un transfer în afara UE prevalează asupra prezentului DPA și a condițiilor de utilizare în chestiunile pe care le reglementează.

## 14. Notificări

---

- Către Dazr: [privacy@dazr.eu](mailto:privacy@dazr.eu) (protecția datelor) sau [security@dazr.eu](mailto:security@dazr.eu) (incidente).

- Către operator: adresa de e-mail a proprietarului spațiului de lucru înregistrată la momentul notificării.