

Anexa GDPR

prelucrarea datelor personale de către DAZOOT SOFTWARE SRL conform GDPR *(Contract prelucrare date personale Operator – Împuternicit Newsman.ro)*

Prezenta anexă prevede regulile specifice în ceea ce privește prelucrarea datelor cu caracter personal trimise de către Beneficiar, în calitate de Operator, de către DAZOOT SOFTWARE SRL, în calitate de împuternicit în conformitate cu Regulamentului (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (denumit în continuare "GDPR"), ca și orice legislație națională subsecventă cu privire la domeniul protecției datelor cu caracter personal.

Art. 1. În cuprinsul acestei anexe termenii folosiți vor fi interpretați în conformitate cu GDPR, iar acolo unde este cazul, termenii folosiți vor avea definițiile stipulate de art. 4 din GDPR.

Art. 2. Obiectul prelucrării datelor personale îl reprezintă prelucrarea de către Împuternicit a datelor personale trimise de către Operator în scopul furnizării serviciilor stipulate în contractul principal de servicii software.

Art. 3. Datele personale puse la dispoziție de către Operator, procesate în temeiul acestui contract sunt:

3.1. Nume, prenume, email, număr de telefon - dacă este cazul - ca și orice date suplimentare încărcate de către Operator direct sau indirect;

3.2. Date și informații legate direct de către email-urile trimise sau acțiuni subsecvente, cum ar fi lista de newsletter deschise sau link-uri accesate (inclusiv marcarea temporală a acestor acțiuni), acțiuni în email (de ex. De-subscriere), adresa IP de la care au provenit acțiunile sau – dacă clientul integrează codul de JS retargeting pus la dispoziție de către Împuternicit – paginile vizitate pe site-ul Operatorului.

Art. 4. Categoriile de persoane vizate sunt abonați și/sau clienți ai Operatorului.

Art. 5. În temeiul acestui contract Operatorul dă următoarele instrucțiuni specifice Împuternicitului:

5.1. Să colecteze și să proceseze date cu caracter personal primite de la Operator în mod direct (prin încărcarea în platforma Împuternicitului) sau indirect (prin intermediul unui formular de abonare al Operatorului). Aceste date sunt cele specificate pe articolul 3.1;

5.2. Să trimită mesaje prin email (newsletter sau mailuri tranzacționale) în numele Operatorului, inclusiv personalizarea acestora, cu conținutul, ora de trimitere și baza de abonați stabilită de către Operator;

5.3. Să colecteze și să proceseze date și informații legate direct de către email-urile trimise sau acțiuni subsecvente, precum cele precizate în art 3.2.;

5.4. Să trimită mesaje prin SMS, cu conținutul, ora de trimitere și baza de abonați stabilită de către Operator, dacă acest serviciu este inclus în contractul principal;

5.5. Orice altă instrucțiune trimisă în scris – electronic sau pe hârtie - de către Operator legată de activitățile prestate conform contractului de servicii software, și pe care Împuternicitul nu o consideră contrară GDPR.

Art. 6. Durata prelucrării datelor cu caracter personal este identică cu durata funcționării contractului principal de furnizare de servicii software.

Art. 7. Natura și scopul prelucrării sunt cele stabilite de către Operator în temeiul contractului principal și anume furnizarea serviciilor de trimitere mesaje email sau SMS, și servicii conexe de analiză și prelucrare a informațiilor legate de aceste mesaje.

Art. 8. În cazul în care prelucrarea datelor Operatorului sau anumite părți ale prelucrării se efectuează de către Împuternicit prin intermediul altor persoane, numite sub-împuterniciți, acesta trebuie să respecte următoarele principii:

8.1. În temeiul acestui articol Operatorul înțelege să autorizeze Împuternicitul să prelucreze datele sale prin următorii sub-împuterniciți pentru următoarele activități:

- Hetzner AG (Germania) - pentru găzduire servere
- Message Bird (Olanda) - pentru găzduire servere SMTP
- Hydra Communication Ltd (UK) - pentru găzduire servere SMTP
- Amazon Web Services EMEA SARL (Luxemburg) - pentru găzduire servere SMTP
- Altmedia Telecom SRL (România) - pentru trimitere SMS
- Any Media Development SRL (România) - pentru trimitere SMS

8.2. Pentru sub-împuterniciți viitori, Împuternicitul primește o autorizare generală de a subcontracta cu orice alt furnizor din U.E., EEA sau țară cu nivel adecvat de protecție recunoscut prin decizie a C.E., care este necesar pentru anumite părți ale procesării datelor conform prezentului contract care oferă un nivel de securitate adecvat, cel puțin la nivelul prezentului contract. Aceasta autorizare include obligația de informare a Operatorului, printr-un mesaj prin contul de pe site-ul Împuternicitului sau prin email. Operatorul are posibilitatea de a formula obiecții în termen de 2 zile lucrătoare.

Art. 9. Drepturile și obligațiile Operatorului

9.1. Dreptul să primească informații sau să verifice, direct sau prin auditor mandatat, modul în care Împuternicitul pune în aplicare măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute de GDPR; verificarea va avea loc în baza unei notificări scrise prealabile, transmisă cu cel puțin 14 zile lucrătoare înainte de efectuarea verificării;

9.2. Dreptul să primească asistență din partea Împuternicitului, în special pentru îndeplinirea obligației sale de a răspunde cererilor persoanelor vizate cu privire la exercitarea drepturilor lor prevăzute de GDPR;

9.3. Dreptul de a face obiecțiuni cu privire la alți sub-împuterniciți conform art. 8.2;

9.4. Să respecte obligațiile sale conform GDPR în calitate de Operator cu privire la datele cu caracter personal colectate sau procesate de Împuternicit, pe seama sa;

9.5. În special să răspundă exclusiv de obținerea acordului persoanelor vizate (sau folosirea altui temei legal) pentru prelucrarea datelor cu caracter personal ce face obiectul prezentului contract, inclusiv în situația în care Împuternicitul este autorizat prin prezentul contract să colecteze datele cu caracter personal în numele Operatorului;

9.6. În toate situațiile în care Operatorul este cel care trebuie să execute o obligație, cum este, spre exemplu, informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal, Împuternicitul nu poate fi ținut de inacțiunile Operatorului din sfera acelei obligații,

Art. 10. Drepturile și obligațiile Împuternicitului:

10.1. Obligația să informeze Operatorul în termen de maxim 10 zile, în cazul în care, în opinia Împuternicitului, o instrucțiune încalcă GDPR și/sau altă dispoziție legală privind prelucrarea datelor cu caracter personal;

10.2. Obligația să asigure securitatea datelor cu caracter personal prelucrate în numele Operatorului în conformitate cu art 32 din GDPR și cu art 11 din prezenta Anexă;

10.3. Obligația de a informa în 48 de ore Operatorul fără întârzieri nejustificate de o încălcare a securității datelor personale ale Operatorului pe parcursul prelucrării realizate de către Împuternicit;

10.4. Obligația de a asista Operatorul cu toate informațiile necesare în vederea notificării, dacă este cazul, către Autoritatea competentă pentru încălcarea securității datelor, dar fără a se substitui Operatorului în obligația sa de notificare;

10.5. Obligația de a acorda asistență Operatorului să asigure respectarea obligațiilor prevăzute la articolele 32-36 din GDPR;

10.6. Obligația de a asista Operatorul pentru soluționarea cererilor persoanelor vizate sau de a transmite Operatorului orice cerere primită de la persoanele vizate, în legătură cu datele personale care au fost colectate și prelucrate de Împuternicit, în termen de maxim 5 zile calendaristice de la primirea acesteia. Această asistență nu se aplică în situația în care Operatorul are deja în instrumentele tehnice furnizate de către Împuternicit posibilitatea de a soluționa cererea persoanei vizate (de ex. de-subscrierea persoanei vizate);

10.7. Obligația să nu transmită date cu caracter personal și/sau informații confidențiale, ce pot fi date cu caracter personal, despre care a luat cunoștință în timpul executării contractului;

10.8. Obligația să asigure instruirea personalului autorizat să prelucreze datele cu caracter personal, cu privire la confidențialitatea acestor date;

10.9. Obligația să includă obligații de confidențialitate către angajați și sub-împunerniciți;

10.10. Dreptul să dezvăluie anumite date cu caracter personal la solicitarea unei autorități, instituții publice sau instanțe judecătorești, ori a unui alt terț autorizat potrivit legislației, în virtutea unei obligații legale sau a unei alte condiții prevăzute de legislație;

10.11. Dreptul de a recruta sub-împunerniciți conform art. 8.1 și 8.2 sau în situația în care a primit aprobare din partea Operatorului;

10.12. Dreptul la acoperirea costurilor generate de asigurarea asistenței Operatorului în situațiile prevăzute de GDPR, dacă acestea depășesc costul lunar al serviciilor prestate de către Împunernicit;

10.13. Dreptul de a folosi informații statistice anonimizate ca urmare a activităților prestate ca urmare a acestui contract sau a întregii sale activități;

10.14. Împunernicitul nu poate stabili scopuri sau mijloace de prelucrare a datelor cu caracter personal, acestea fiind stabilite exclusiv de către Operator.

Art. 11. Împunernicitul a stabilit aplicarea internă a următoarele măsuri organizatorice și tehnice de securitate pentru securitatea datelor personale, luând în considerare tipul de activitate prestată:

- Instruire periodică personal (politică internă de securitate)
- Acces birou pe bază de cheie și / sau smart lock (Nuki)
- Stații de lucru cu hard disk-uri criptate
- Stocare de date cu caracter personal exclusiv în datacenter (nu se stochează nimic la birou)
- Acces backend SSL (secure) doar folosind autentificare în 2 pași
- Acces angajaților în backend este limitat (nu văd datele cu caracter personal încărcate de operator)
- Acces servere via VPN + SSH Agent (chei RSA 2048 biți, stocate exclusiv pe hard disk-urile criptate)
- Servere securizate (update-uri la zi + rulare IDS - intrusion detection system)
- Servere cu firewall restrictiv

Securizare aplicație Newsman:

- Access exclusiv SSL (secure)
- Autentificare în 2 pași (login)
- Opțiuni sub accounts (conturi cu acces restrictiv la aplicație, ex: doar read sau doar editor, fără opțiuni de download baza de date)
- Protecție brute force (lock IP după câteva încercări eșuate)
- Parole strong (minim 10 caractere, o literă mare, o literă mica, un caracter special)
- Protecție session high jacking (session capture)
- Protecție CSRF / XSS
- High Security Mode (reintroducere cod autentificare în 2 pași) necesar pentru acces zone sensibile din aplicație (ex: vizualizare adrese de mail sau modificare profil sau download baze de date - expiră în 4 ore de la activare)

- Notificări download, link-uri ce expiră în 4 ore, logging extensiv downloads
- Notificări logare IP nou / țară nouă (dacă nu este activată autentificarea în 2 pași)
- Notificare modificare parolă sau date profil (dacă nu este activată autentificarea în 2 pași)
- Scanare vulnerabilități aplicație lunare

Aceste măsuri sunt centralizate în cadrul Politicii interne de securitate interne, care poate fi pusă de dispoziție la cerere.

Art. 12. Operatorul este de acord să exonereze Împuternicitul de orice răspundere pentru pagubele ce ar putea decurge din:

12.1. nerespectarea contractului din cauza unor evenimente ce exced oricărei răspunderi a Împuternicitului;

12.2. respectarea instrucțiunilor Operatorului sau nerespectarea instrucțiunilor Operatorului justificată în prealabil printr-o notificare referitoare la nelegalitatea ei;

12.3. lipsa sau vicierea acordului persoanelor vizate sau a utilizării unui temei legal greșit de către Operator; nerespectarea contractului din cauza unor acțiuni ale Operatorului.

Art. 13. Această anexă intră în vigoare pe 25 mai 2018.

Furnizor
(Împuternicit)
SC Dazoot Software SRL

Beneficiar
(Operator)

Administrator,
Cătălin Constantin

Administrator,