

|                                           |          |
|-------------------------------------------|----------|
| <b>Politica de Confidențialitate.....</b> | <b>1</b> |
| <b>Privacy Policy .....</b>               | <b>5</b> |

## **Politica de Confidențialitate**

Data publicării: 07.10.2025

*Întocmită de AI Professional Software Solutions SRL, CUI 12345678, înregistrată la Registrul Comerțului sub numărul J39/1234/2015, cu sediul în Municipiul Piatra Neamț, județul Neamț, strada Iulian Antonescu, nr. 4, bl. T5, ap.15 (denumită în continuare „Compania”)*

### **0. Definiții și termeni utilizați**

În sensul prezentei Politici de confidențialitate, termenii utilizați au următoarele semnificații, în conformitate cu prevederile Regulamentului (UE) 2016/679 (GDPR):

- **„Date cu caracter personal”** – orice informație care permite identificarea directă sau indirectă a unei persoane fizice, cum ar fi numele, prenumele, adresa de e-mail, numărul de telefon, adresa IP, identificatori de dispozitiv, date de localizare, date conținute în cererile transmise prin platformă etc.
- **„Prelucrarea datelor cu caracter personal”** – orice operațiune efectuată asupra datelor, cum ar fi colectarea, înregistrarea, organizarea, stocarea, modificarea, utilizarea, transmiterea, divulgarea, arhivarea sau ștergerea acestora.
- **„Operator”** – entitatea care stabilește scopurile și mijloacele prelucrării datelor cu caracter personal. În contextul prezentei politici, operatorul este **AI Professional Software Solutions SRL**, în calitate de administrator al platformei **Gov-Smart**.
- **„Persoană vizată”** – orice persoană fizică ale cărei date cu caracter personal sunt prelucrate prin intermediul platformei (de exemplu, utilizatori, funcționari publici, cetățeni care transmit solicitări către autorități).
- **„Persoană împuternicită” (procesator)** – o terță parte care prelucrează date personale în numele Operatorului, pe baza unui contract (de exemplu, furnizori de servicii IT, găzduire, suport tehnic etc.).

- **„Consimțământ”** – orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate, prin care persoana vizată își exprimă acordul pentru prelucrarea datelor sale cu caracter personal.
- **„Autoritate de supraveghere”** – Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) din România sau o autoritate competentă din alt stat membru al Uniunii Europene.
- **„Serviciile platformei”** – totalitatea funcționalităților puse la dispoziție prin intermediul site-ului și aplicațiilor Gov-Smart, inclusiv formularele electronice, spațiul de comunicare dintre cetățeni și instituțiile publice, precum și modulele opționale utilizate de autorități.
- **„Cookie-uri” / „Date tehnice”** – fișiere și informații tehnice colectate automat atunci când utilizați platforma, care pot include adresa IP, tipul de browser, durata sesiunii, identificatori de dispozitiv sau alte date similare.

## 1. Introducere

Această politică descrie ce informații colectăm atunci când utilizați platforma Gov-Smart, aplicațiile și serviciile sale („Servicii”), cum le stocăm, utilizăm, transferăm și ștergem, precum și ce opțiuni aveți în legătură cu aceste informații.

Această politică se aplică tuturor interacțiunilor cu Gov-Smart, inclusiv site-ul web, aplicațiile mobile și interacțiunile directe cu reprezentanții Companiei.

Compania acționează ca Operator de date cu caracter personal pentru datele personale ale utilizatorilor serviciilor noastre, ceea ce înseamnă că determinăm scopurile și mijloacele procesării datelor personale. Pentru conținutul pe care îl încărcăți sau îl puneți la dispoziție prin intermediul serviciilor („Conținut utilizator”), sunteți responsabil să vă asigurați că acesta respectă Termenii și Condițiile platformei și nu încalcă drepturile altor utilizatori.

## 2. Cum colectăm, procesăm și stocăm datele

Compania colectează și prelucrează datele necesare pentru a vă oferi și menține serviciile Gov-Smart. Tipurile de date includ:

- Informații de identificare:** nume, prenume, adresă de e-mail, telefon sau funcție.
- Date de utilizare:** adresa IP, locația geografică, tipul și versiunea browser-ului, sistemul de operare, durata sesiunilor și navigarea în platformă.
- Date tehnice (log-uri):** informații colectate automat de servere (IP, user-agent, timestamp, endpoint accesat, cod de răspuns HTTP – 200/400/500).
- Cookie-uri:** doar cookie-uri strict tehnice, necesare pentru autentificare și menținerea sesiunilor active; nu se folosesc cookie-uri de marketing sau analiză.
- Informații despre dispozitive:** tipul dispozitivului, sistemul de operare, identificatori unici de dispozitiv.

- f. **Informații din activități de suport:** date furnizate prin cereri de asistență sau comunicare cu echipa Gov-Smart.
- g. **Notificări privind serviciile:** date utilizate pentru a vă informa despre modificări ale Termenilor și Condițiilor sau activități suspecte pe cont.
- h. **Integrări cu servicii externe:** date privind utilizarea serviciilor partenerilor pentru îmbunătățirea experienței utilizatorului, stocate temporar sau permanent în funcție de tipul de integrare.

Datele sunt colectate direct de la utilizator, prin formulare electronice sau interacțiuni cu platforma.

Transmiterea se face în mod securizat, prin conexiuni **criptate (HTTPS)**, către infrastructura Microsoft Azure (centre de date situate în Uniunea Europeană). Toate datele sunt stocate în baze de date **PostgreSQL** securizate și criptate la nivel de disc. Accesul la date este limitat pe baza principiului „**need-to-know**”, doar personalului autorizat. Logurile tehnice (de erori și request-uri HTTP) sunt transmise către un serviciu **self-hosted de tip Datadog**, unde sunt păstrate **maximum 3 luni**. Tabelul intern de audit al platformei (pentru trasabilitate) este **permanent**, dar intrările sunt **anonimizate** atunci când se solicită ștergerea datelor asociate unui utilizator.

Nu există **ștergere automată** a datelor utilizatorilor. La cererea expresă a utilizatorului, datele sunt **marcate pentru ștergere logică**, devenind inaccesibile din platformă și excluse din fluxurile de prelucrare. În cazurile în care datele trebuie păstrate pentru motive legale sau de audit, acestea sunt **anonimizate** ireversibil. Backup-urile bazei de date se realizează periodic și sunt criptate; accesul este restricționat.

### 3. Cum procesăm elementele media

Gov-Smart poate colecta și stoca conținut media (de exemplu, capturi, înregistrări sau documente de identificare) **numai cu acordul explicit al utilizatorului** și exclusiv în scopurile permise de lege, cum ar fi: verificarea identității; prevenirea fraudelor sau accesului neautorizat și asigurarea securității platformei.

Datele media sunt păstrate **pe durata utilizării serviciilor**, sau **până la finalizarea verificărilor** în cazul unor suspiciuni de identitate sau acces neautorizat. După îndeplinirea scopului pentru care au fost colectate, datele media sunt **anonimizate sau șterse la cererea utilizatorului**, conform politicii interne de retenție.

### 4. Securitate

Compania implementează măsuri tehnice și organizaționale pentru protecția datelor împotriva accesului neautorizat, pierderii sau deteriorării.

Comunicațiile între utilizatori se pot face peer-to-peer sau prin serverele Companiei, care sunt protejate cu măsuri stricte de securitate.

## **5. Accesul altor entități la datele personale**

Datele pot fi dezvăluite în următoarele situații:

- Cu consimțământul utilizatorului;
- Partenerilor, licențiatorilor, furnizorilor și afiliaților noștri pentru buna funcționare a serviciilor care sunt obligați să se conformeze politicii de confidențialitate a SC AI Professional Software Solutions SRL;
- La cererea autorităților, conform legii.

**Tipuri de parteneri/furnizori:** infrastructură și găzduire, procesatori de plăți, furnizori de semnături electronice, instrumente de colaborare, suport clienți, marketing și comunicare, analiză tehnică a platformei.

## **6. Păstrarea și ștergerea datelor**

Datele personale sunt păstrate doar cât timp este necesar scopurilor pentru care au fost colectate:

- Datele vor fi păstrate pe un termen nelimitat, dar cu posibilitatea de a fi șterse sau anonimizate la cerere. În cazul în care există prevederi legale care să ne oblige altfel, vor fi respectate prevederile legale.

## **7. Modificarea acestei politici**

Compania poate modifica politica oricând.. Continuarea utilizării platformei după modificări implică acceptul utilizatorului.

## **8. Drepturile utilizatorului**

Utilizatorii au drepturi conform legislației naționale și europene:

- Dreptul de acces la datele personale;
- Dreptul la rectificarea datelor;
- Dreptul de opoziție și restricționare a prelucrării;
- Dreptul la ștergerea datelor („dreptul de a fi uitat”);
- Dreptul la portabilitatea datelor;
- Dreptul de a depune o plângere la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) sau la o autoritate de supraveghere din alt stat membru UE în care persoana vizată își are reședința.

## 9. Persoana responsabilă cu protecția datelor

Compania a desemnat o persoană responsabilă cu protecția datelor cu caracter personal, care poate fi contactată pentru orice întrebări, clarificări sau exercitarea drepturilor utilizatorilor în legătură cu datele personale:

**Nume:** Robert Marin

**Funcție:** Responsabil cu protecția datelor / Data Protection Officer

**Email:** [office@aipss.com](mailto:office@aipss.com)

Persoana responsabilă se asigură că datele utilizatorilor sunt procesate conform legislației aplicabile și poate gestiona cereri privind accesul, rectificarea, ștergerea sau restricționarea datelor.

Pentru a vă exercita drepturile privind datele cu caracter personal sau pentru orice alte întrebări legate de modul în care acestea sunt procesate, vă rugăm să ne contactați la adresa de email **office@aipss.com**. De asemenea, aveți posibilitatea de a depune sesizări sau reclamații direct la Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) sau la o autoritate de supraveghere din alt stat membru UE în care persoana vizată își are reședința.

## Privacy Policy

**Publication Date:** October 7, 2025

Prepared by **AI Professional Software Solutions SRL**, VAT no. 12345678, registered with the Trade Register under no. J39/1234/2015, with its registered office in Piatra Neamț Municipality, Neamț County, Iulian Antonescu Street no. 4, Building T5, Apartment 15 (hereinafter referred to as the “Company”).

### 0. Definitions and Terms

For the purposes of this Privacy Policy, the following terms have the meanings set forth below, in accordance with Regulation (EU) 2016/679 (“GDPR”):

**“Personal data”** – any information that allows the direct or indirect identification of a natural person, such as name, surname, email address, phone number, IP address, device identifiers, location data, or data included in requests submitted through the platform.

**“Processing of personal data”** – any operation performed on personal data, such as collection, recording, organization, storage, modification, use, transmission, disclosure, archiving, or deletion.

**“Controller”** – the entity that determines the purposes and means of processing personal data. In the context of this Policy, the Controller is **AI Professional Software Solutions SRL**, as administrator of the Gov-Smart platform.

**“Data subject”** – any natural person whose personal data are processed through the platform (for example: users, public officials, citizens submitting requests to authorities).

**“Processor”** – a third party that processes personal data on behalf of the Controller, based on a contract (for example: IT service providers, hosting providers, technical support partners, etc.).

**“Consent”** – any freely given, specific, informed, and unambiguous indication of the data subject’s wishes by which they signify agreement to the processing of their personal data.

**“Supervisory authority”** – the **National Supervisory Authority for Personal Data Processing (ANSPDCP)** in Romania or another competent authority in an EU Member State.

**“Platform services”** – all functionalities made available through the Gov-Smart website and applications, including electronic forms, communication spaces between citizens and public institutions, and optional modules used by authorities.

**“Cookies” / “Technical data”** – files and technical information automatically collected when you use the platform, which may include IP address, browser type, session duration, device identifiers, or similar data.

## **1. Introduction**

This Policy describes the information we collect when you use the **Gov-Smart** platform, applications, and services (“Services”), how we store, use, transfer, and delete that information, and what options you have regarding it.

This Policy applies to all interactions with Gov-Smart, including the website, mobile applications, and direct communications with the Company’s representatives.

The Company acts as **Data Controller** for the personal data of users of our services, meaning we determine the purposes and means of processing such data. For content that you upload or make available through the Services (“User Content”), you are responsible for ensuring compliance with the Platform’s **Terms and Conditions** and for not infringing upon the rights of other users.

## 2. How We Collect, Process, and Store Data

The Company collects and processes data necessary to provide and maintain the Gov-Smart Services. Types of data include:

- **Identification data:** name, surname, email address, phone number, or position/title.
- **Usage data:** IP address, geographic location, browser type and version, operating system, session duration, and navigation activity within the platform.
- **Technical data (logs):** information automatically collected by servers (IP, user-agent, timestamp, accessed endpoint, HTTP response code – 200/400/500).
- **Cookies:** strictly technical cookies necessary for authentication and maintaining active sessions; no marketing or analytics cookies are used.
- **Device information:** device type, operating system, and unique device identifiers.
- **Support activity data:** information provided through assistance requests or communications with the Gov-Smart support team.
- **Service notifications:** data used to inform you about changes to the Terms and Conditions or about suspicious account activity.
- **External integrations:** data regarding the use of partner services to improve the user experience, stored temporarily or permanently depending on the type of integration.

Data is collected directly from the user, via electronic forms or interactions with the platform.

Transmission is performed securely through encrypted connections (HTTPS) to the **Microsoft Azure** infrastructure (data centers located in the European Union). All data is stored in **encrypted PostgreSQL databases** with disk-level encryption. Access is restricted on a “need-to-know” basis and granted only to authorized personnel.

Technical logs (errors and HTTP requests) are transmitted to a **self-hosted Datadog-like service**, where they are retained for a maximum of 3 months. The internal audit table (for traceability) is permanent, but entries are anonymized when a user’s data is deleted upon request.

There is **no automatic deletion** of user data. Upon explicit user request, data are marked for logical deletion, becoming inaccessible within the platform and excluded from processing flows. When data must be retained for legal or audit purposes, they are irreversibly anonymized. Database backups are performed periodically, encrypted, and access to them is strictly restricted.

## 3. Processing of Media Elements

Gov-Smart may collect and store media content (such as captures, recordings, or identification documents) **only with the user’s explicit consent** and solely for legally permitted purposes, such as:

- identity verification;

- prevention of fraud or unauthorized access;
- ensuring platform security.

Media data are retained for the duration of service use or until identity or security verifications are completed.

After the purpose has been fulfilled, media data are anonymized or deleted upon the user's request, in accordance with the internal data retention policy.

#### **4. Security**

The Company implements appropriate **technical and organizational measures** to protect data against unauthorized access, loss, or damage.

Communications between users may occur **peer-to-peer** or via the Company's servers, which are protected by strict security measures.

#### **5. Access of Other Entities to Personal Data**

Data may be disclosed in the following cases:

- With the user's consent;
- To our partners, licensors, suppliers, and affiliates necessary for proper service operation, all of whom are required to comply with the privacy standards of AI Professional Software Solutions SRL;
- At the request of public authorities, in accordance with applicable law.

**Types of partners/providers:** Infrastructure and hosting services, payment processors, electronic signature providers, collaboration tools, customer support, marketing and communication services, and technical analysis providers.

#### **6. Data Retention and Deletion**

- The data related to usage and personal content will be retained for an unlimited period, but may be deleted or anonymized upon request, within 5 years from creation.

In cases where legal provisions require otherwise, those legal requirements will be fully respected.

#### **7. Changes to This Policy**

The Company may amend this Policy at any time. Continued use of the platform after such modifications constitutes acceptance of the updated version by the user.

## 8. User Rights

Users have the following rights under national and European data protection laws:

- **Right of access** to personal data;
- **Right to rectification** of inaccurate or incomplete data;
- **Right to object** to and restrict processing;
- **Right to erasure** (“right to be forgotten”);
- **Right to data portability**;
- **Right to lodge a complaint** with the **National Supervisory Authority for Personal Data Processing (ANSPDCP)** or with a supervisory authority in another EU Member State where the data subject resides.

## 9. Data Protection Officer

The Company has appointed a **Data Protection Officer (DPO)** who can be contacted for any questions, clarifications, or to exercise your rights regarding personal data:

**Name:** Robert Marin

**Position:** Data Protection Officer

**Email:** [office@aipss.com](mailto:office@aipss.com)

The DPO ensures that users’ data are processed in accordance with applicable legislation and handles requests related to access, rectification, deletion, or restriction of data.

To exercise your data protection rights or for any other inquiries regarding the processing of personal data, please contact us at [office@aipss.com](mailto:office@aipss.com). You may also file complaints directly with the **National Supervisory Authority for Personal Data Processing (ANSPDCP)** or with a competent supervisory authority in another EU Member State where you reside.