CODUL DE CONDUITĂ ȘI ETICĂ ÎN AFACERI

(CODE OF BUSINESS CONDUCT AND ETHICS)

CODATA SOFTWARE SOLUTIONS

Versiune aprobată, Septembrie 2025

CUPRINS

MESAJUL MANAGEMENTULUI
I. Generalități
II. Managementul riscului reputațional
III. Politica anti-mită și anti-corupție
IV. Politica privind prevenirea și combaterea spălării banilor și a finanțării terorismului
V. Politica privind concurența
VI. Politica privind confidențialitatea și protecția informațiilor
VII. Politica de prevenire a fraudei interne
VIII. Politica de conduită și comportament în CODATA
IX. Politica de avertizare și anti-represalii (Speak-Up)
X. Politica privind guvernanța ESG
XI. Politica de conformitate cu comerțul global și reglementările internaționale
XII. Dispoziții finale

MESAJUL MANAGEMENTULUI

Dragi colegi, parteneri și colaboratori,

Etica în afaceri, transparența și responsabilitatea corporativă reprezintă fundamentul pe care CODATA Software Solutions și-a construit reputația. Într-un domeniu dinamic, în care tehnologia și încrederea merg mână în mână, conduita noastră etică determină nu doar succesul comercial, ci și valoarea pe care o aducem societății.

De la primele proiecte de digitalizare până la soluțiile bazate pe inteligență artificială și cloud, ne-am ghidat constant după principii clare: integritate, profesionalism, respect și responsabilitate. Fiecare decizie de business trebuie luată cu onestitate, cu respect față de lege și față de partenerii noștri.

„Codul de Conduită și Etică în Afaceri" al CODATA stabilește principiile pe care le urmăm în toate activitățile noastre, în România și în afara țării. Este o expresie a culturii noastre organizaționale și un angajament față de toți cei cu care colaborăm: clienți, instituții, parteneri, colegi și comunitate.

Integritatea și transparența sunt pilonii de încredere în relațiile cu partenerii noștri strategici și instituțiile publice naționale. Respectarea celor mai înalte standarde de conformitate nu este o opțiune, ci o obligație profesională.

Reputația CODATA este o resursă esențială. O singură abatere poate afecta imaginea întregii organizații. De aceea, fiecare angajat și partener CODATA trebuie să fie un exemplu de corectitudine și responsabilitate, acționând cu integritate indiferent de context.

Cultura noastră organizațională se bazează pe curajul de a spune adevărul, pe deschidere și pe capacitatea de a învăța continuu. Încurajăm o atitudine proactivă, raportarea oricărei situații neetice și colaborarea permanentă pentru a menține un climat sănătos și sigur.

Integritatea nu este o formalitate. Este o alegere zilnică. Este modul în care construim viitorul CODATA, o companie de încredere, partener al transformării digitale și al progresului bazat pe etică, inovație și responsabilitate.

Horia SABO
Director general
CODATA Software Solutions
București, Septembrie 2025

MESSAGE FROM THE MANAGEMENT

Dear colleagues, partners, and collaborators,

Business ethics, transparency, and corporate responsibility are the foundation upon which CODATA Software Solutions has built its reputation. In a dynamic field where technology and trust go hand in hand, our ethical conduct determines not only commercial success but also the value we bring to society.

From our first digital transformation projects to today's AI and cloud-based solutions, we have remained guided by clear principles: integrity, professionalism, respect and accountability. Every business decision must be made honestly, in full compliance with the law and with respect for our partners.

The **CODATA Code of Business Conduct and Ethics** defines the standards we uphold in all our activities, both in Romania and internationally. It is an expression of our organizational culture and a commitment to everyone we work with clients, institutions, partners, colleagues, and the broader community.

Integrity and transparency are the cornerstones of our relationships with strategic and national public institutions. Upholding the highest standards of compliance is not optional; it is our professional duty.

CODATA's reputation is one of our most valuable assets. A single lapse in judgment can affect the entire organization. This is why every employee and partner must act with honesty, responsibility, and integrity in every situation.

Our organizational culture is built on openness, courage, and continuous learning. We encourage every member of our team to speak up, report unethical behavior, and collaborate to maintain a safe and fair working environment.

Integrity is not a formality. It is a daily choice. It is how we build the future of CODATA a trusted company, a driver of digital transformation, and a promoter of ethical, innovative, and responsible technology.

Horia SABO
General manager
CODATA Software Solutions
Bucharest, September 2025

I. GENERALITĂȚI

1. Scopul Codului

Acest **Cod de Conduită și Etică în Afaceri** definește principiile, valorile și regulile fundamentale care ghidează activitatea CODATA Software Solutions. Scopul său este de a asigura o cultură organizațională bazată pe integritate, transparență, profesionalism și respect pentru lege, clienți și angajați.

Codul stabilește standardele minime de comportament etic și profesional, aplicabile tuturor persoanelor care acționează în numele CODATA, angajați, consultanți, colaboratori, furnizori și parteneri.

Prin adoptarea acestui Cod, compania își reafirmă angajamentul față de:

- o conduită corectă și responsabilă;
- respectarea legislației naționale și internaționale;
- conformitatea cu reglementările privind protecția datelor, concurența, anticorupția, mediul și guvernanța corporativă;
- promovarea unei culturi a încrederii, transparenței și colaborării.

2. Domeniul de aplicare

Codul se aplică:

- tuturor angajaților CODATA, indiferent de funcție, poziție sau locație;
- tuturor partenerilor de afaceri, subcontractorilor, consultanților și furnizorilor care acționează în numele CODATA;
- filialelor și entităților afiliate la nivel național și internațional.

Respectarea acestui Cod este o condiție esențială pentru apartenența la organizație și pentru menținerea oricărei forme de colaborare contractuală cu CODATA Software Solutions.

3. Principii fundamentale

Activitatea CODATA este guvernată de următoarele principii de etică profesională:

1. **Integritate** – acționăm onest și transparent în toate relațiile de afaceri.
2. **Responsabilitate** – respectăm legile, angajamentele și valorile noastre.
3. **Transparență** – comunicăm clar, corect și complet cu toate părțile implicate.
4. **Respect** – tratăm fiecare persoană cu demnitate și echitate.
5. **Inovație etică** – dezvoltăm și implementăm tehnologii digitale și AI într-un mod responsabil, sigur și conform normelor morale și legale.
6. **Conformitate** – aplicăm cele mai stricte standarde de guvernanță corporativă și securitate a informației.

4. Valorile CODATA

Valorile noastre definesc cultura organizațională și comportamentul zilnic al echipei:

- **Profesionalism** – fiecare decizie se bazează pe competență, calitate și rigoare.
- **Încredere** – respectăm promisiunile făcute clienților și partenerilor.
- **Colaborare** – lucrăm împreună, deschis, pentru rezultate durabile.
- **Inovație responsabilă** – folosim tehnologia pentru a genera progres, fără a compromite etica sau securitatea.
- **Respect pentru lege și parteneri** – conformitatea este o parte centrală a succesului nostru.

5. Responsabilități individuale

Fiecare membru al echipei CODATA are obligația de a:

- cunoaște și aplica prevederile Codului;
- evita orice acțiune care ar putea compromite integritatea companiei;
- raporta imediat orice comportament neetic sau ilegal;
- proteja interesele și reputația organizației.

Ignoranța nu este o scuză. Orice abatere de la prezentul Cod poate conduce la măsuri disciplinare, inclusiv încetarea colaborării.

I. GENERAL PRINCIPLES

1. Purpose of the Code

This **Code of Business Conduct and Ethics** defines the principles, values, and behavioral standards guiding the activity of CODATA Software Solutions. Its purpose is to promote a corporate culture rooted in integrity, transparency, professionalism, and respect for law, clients, and employees.

The Code establishes the minimum ethical and professional standards applicable to all individuals acting on behalf of CODATA employees, consultants, contractors, suppliers, and partners.

By adopting this Code, CODATA reaffirms its commitment to:

- ethical and responsible business conduct;
- compliance with national and international laws;
- adherence to regulations on data protection, competition, anti-corruption, environment, and corporate governance;
- fostering a culture of trust, transparency, and collaboration.

2. Scope

This Code applies to:

- all employees of CODATA, regardless of role, seniority, or location;
- all business partners, subcontractors, consultants, and suppliers acting on behalf of CODATA;
- all subsidiaries and affiliated entities, both domestic and international.

Compliance with this Code is a fundamental condition for employment or collaboration with CODATA Software Solutions.

3. Core Principles

CODATA's operations are guided by the following principles:

1. **Integrity** – acting honestly and transparently in all business relations.
2. **Accountability** – complying with laws, commitments, and organizational values.
3. **Transparency** – communicating openly and accurately with all stakeholders.
4. **Respect** – treating all individuals with dignity and fairness.
5. **Ethical Innovation** – developing and deploying digital and AI technologies responsibly, safely, and lawfully.
6. **Compliance** – adhering to strict governance, security, and ethical standards.

4. CODATA Values

Our values define who we are and how we act every day:

- **Professionalism** – making decisions based on expertise and quality.

- **Trust** – honoring commitments made to clients and partners.
- **Collaboration** – working together with openness and purpose.
- **Responsible Innovation** – leveraging technology to advance society without compromising ethics or security.
- **Respect for Law and Partners** – compliance as a foundation of sustainable success.

5. Individual Responsibilities

Every member of CODATA must:

- understand and apply this Code;
- avoid any conduct that could damage the company's integrity;
- promptly report unethical or illegal actions;
- protect the organization's interests and reputation.

Ignorance is not an excuse. Any violation of this Code may result in disciplinary measures, including termination of collaboration.

II. MANAGEMENTUL RISCULUI REPUTAȚIONAL

1. Importanța reputației corporative

Reputația CODATA Software Solutions este una dintre cele mai valoroase resurse ale companiei. Ea reflectă încrederea pe care clienții, partenerii, instituțiile publice și comunitatea o au în competența, etica și seriozitatea noastră. Orice acțiune individuală poate consolida sau, dimpotrivă, afecta imaginea întregii organizații.

Reputația nu se construiește prin campanii de comunicare, ci prin fapte, prin consistență și prin decizii corecte, luate zi de zi.

De aceea, fiecare angajat, consultant sau partener CODATA este responsabil pentru modul în care se reflectă valorile companiei în activitatea sa profesională.

2. Principii de gestionare a riscului reputațional

Pentru protejarea imaginii și a încrederii publice, CODATA aplică următoarele principii fundamentale:

1. **Integritate totală** – fiecare acțiune trebuie să fie etică, legală și transparentă.
2. **Responsabilitate colectivă** – reputația este un bun comun, apărat prin comportamente individuale corecte.
3. **Transparență și comunicare echilibrată** – toate mesajele publice trebuie să fie corecte, verificabile și aprobate conform procedurilor interne.
4. **Respectarea confidențialității** – informațiile interne, contractuale sau sensibile nu pot fi comunicate fără autorizare.
5. **Reacție rapidă și profesionistă** – orice incident care poate afecta imaginea companiei este tratat imediat, documentat și comunicat corespunzător.

3. Zone de risc reputațional

CODATA monitorizează permanent factorii care pot influența negativ percepția publică, printre care:

- nerespectarea obligațiilor contractuale sau a termenelor;
- incidente de securitate informatică sau pierderi de date;
- conflicte de interese nedeclarate;
- comportamente neetice, discriminare, hărțuire sau abuz de autoritate;
- parteneriate cu entități neconforme sau implicate în activități ilegale;
- declarații publice neautorizate despre clienți, instituții sau proiecte;
- lipsa de conformitate cu standardele de mediu, protecția datelor sau reglementările EU.

4. Prevenire și monitorizare

CODATA implementează un sistem integrat de prevenire a riscurilor reputaționale, care include:

- **proceduri interne de conformitate** (ISO 37001, ISO 27001, GDPR, NIS2);
- **evaluarea partenerilor și subcontractorilor** din perspectiva eticii, securității și legalității;

- **mecanisme de raportare internă (speak-up)** pentru sesizarea oricăror nereguli;
- **traininguri anuale de etică și conformitate** pentru tot personalul;
- **plan de comunicare de criză**, coordonat de Departamentul de Conformitate și PR.

5. Responsabilități

Responsabilitatea pentru gestionarea riscului reputațional revine:

- **Consiliului de Administrație**, care definește politicile generale;
- **Directorului de Conformitate**, care monitorizează implementarea procedurilor și gestionează incidentele;
- **Departamentului de Comunicare**, care coordonează mesajele externe;
- **Fiecărui angajat**, care trebuie să acționeze conform principiilor Codului, evitând orice comportament care ar putea afecta imaginea companiei.

II. REPUTATIONAL RISK MANAGEMENT

1. Importance of Corporate Reputation

The reputation of CODATA Software Solutions is one of its most valuable strategic assets. It represents the trust that clients, partners, public institutions, and the community place in our competence, ethics, and reliability. Every individual action has the potential to strengthen or damage the company's image.

Reputation is not built through communication campaigns but through consistent ethical behavior and sound decisions made daily.

Therefore, each employee, consultant, and partner shares responsibility for how CODATA's values are reflected in their professional conduct.

2. Principles of Reputational Risk Management

To protect its image and public trust, CODATA applies the following core principles:

1. **Total Integrity** – every action must be ethical, legal, and transparent.
2. **Collective Responsibility** – reputation is a shared asset preserved through individual accountability.
3. **Transparent Communication** – all public messages must be accurate, verified, and internally approved.
4. **Confidentiality** – internal or sensitive information must never be disclosed without authorization.
5. **Swift and Professional Response** – any incident with potential reputational impact is handled immediately, documented, and communicated properly.

3. Areas of Reputational Risk

CODATA continuously monitors risks that could negatively affect its reputation, including:

- failure to meet contractual or delivery obligations;
- cybersecurity breaches or data loss;
- undisclosed conflicts of interest;
- unethical conduct, discrimination, harassment, or abuse of authority;
- partnerships with non-compliant or legally compromised entities;
- unauthorized public statements about clients, institutions, or projects;
- non-compliance with environmental, data protection, or NATO/EU security standards.

4. Prevention and Monitoring

CODATA has established an integrated system for preventing and managing reputational risks, which includes:

- **internal compliance frameworks** (ISO 37001, ISO 27001, GDPR, NIS2);
- **partner and subcontractor due diligence** focusing on ethics, security, and legality;

- **internal reporting channels (speak-up system)** for any suspected irregularities;
- **annual ethics and compliance training** for all employees;
- **a crisis communication plan** coordinated by the Compliance and PR departments.

5. Responsibilities

Responsibility for reputational risk management lies with:

- **The Board of Directors**, which defines general policies;
- **The Compliance Director**, who oversees implementation and incident management;
- **The Communication Department**, which manages all external messaging;
- **Every employee**, who must act according to this Code and avoid any behavior that could damage the company’s image.

III. POLITICA ANTI-MITĂ ȘI ANTI-CORUPȚIE

1. Scopul politicii

Scopul acestei politici este de a preveni, identifica și elimina orice formă de mită, corupție sau comportament neetic în cadrul activităților CODATA Software Solutions. Compania aplică o **politică de toleranță zero** față de orice acțiune care ar putea fi interpretată ca tentativă de corupție, influență nejustificată sau avantaj necuvenit.

Această politică completează principiile stabilite prin Codul de Conduită și Etică în Afaceri și este obligatorie pentru toți angajații, partenerii, consultanții și subcontractorii CODATA.

2. Definiții

- **Mită:** orice ofertă, promisiune, plată, cadou, favor, avantaj material sau nematerial oferit pentru a influența decizia unei persoane într-un mod necorespunzător.
- **Corupție:** folosirea poziției sau funcției pentru obținerea unui beneficiu personal sau de grup, în schimbul unor favoruri, informații sau contracte.
- **Funcționar public:** orice persoană care deține o funcție într-o instituție de stat, organizație internațională sau companie deținută parțial de stat.
- **Comision neautorizat:** plată disimulată sau nejustificată, efectuată pentru a obține un contract, o decizie sau un avantaj comercial.

3. Principii generale

CODATA respectă legislația națională și internațională privind prevenirea și combaterea corupției, inclusiv:

- Legea nr. 78/2000 privind prevenirea faptelor de corupție;
- Foreign Corrupt Practices Act (SUA);
- UK Bribery Act (Marea Britanie);
- Directiva (UE) 2017/1371 privind protejarea intereselor financiare ale Uniunii Europene.

Toate activitățile CODATA se desfășoară cu transparență, integritate și responsabilitate față de clienți, instituții și parteneri.

4. Interdicții explicite

Sunt strict interzise următoarele acțiuni:

1. Oferirea, promisiunea sau acceptarea de bani, bunuri, servicii sau avantaje necuvenite.
2. Solicitarea sau primirea de cadouri, donații sau sponsorizări în scopul influențării deciziilor.
3. Utilizarea intermediarilor sau consultanților pentru a disimula plăți ilegale.
4. Plata de „facilități” (facilitation payments) către funcționari publici, indiferent de valoare.
5. Orice tip de donație, contribuție politică sau sponsorizare care poate fi percepută ca mijloc de influențare.

6. Angajarea rudelor sau apropiaților unui partener de afaceri sau funcționar public fără o evaluare transparentă.
7. Orice formă de complicitate, tăinuire sau neglijență intenționată față de acte de corupție.

5. Cadouri și ospitalitate

CODATA permite doar gesturi simbolice de curtoazie, cu valoare modestă, rezonabilă și transparentă, care:

- nu influențează și nu pot fi interpretate ca influențând o decizie;
- sunt conforme cu uzanțele de afaceri și reglementările interne;
- sunt raportate și aprobate de management înainte de oferire sau acceptare.

Cadourile, mesele de protocol sau invitațiile la evenimente nu trebuie să depășească limitele de bun-simț și trebuie înregistrate în registrul intern de conformitate.

6. Relațiile cu funcționarii publici și partenerii instituționali

În toate interacțiunile cu autorități naționale, europene sau internaționale, CODATA:

- respectă procedurile legale și canalele oficiale de comunicare;
- documentează toate întâlnirile, contractele și corespondența;
- interzice oferirea oricărui avantaj personal sau financiar;
- aplică principiul „transparenței totale" pentru toate proiectele finanțate din fonduri publice sau europene.

7. Plăți și comisioane

Toate plățile efectuate de CODATA trebuie:

- să fie justificate printr-un contract legal;
- să aibă documente suport clare (facturi, rapoarte, dovezi de livrare);
- să fie autorizate conform procedurilor interne.

Sunt interzise plățile în numerar, plățile către conturi personale și tranzacțiile neînregistrate în sistemul contabil oficial.

8. Raportare și protecția avertizorilor

Orice suspiciune de mită, comision ilegal sau act de corupție trebuie raportată imediat prin canalele oficiale:

- **Email dedicat:** compliance@codata.ro
- **Linie internă de etică (Speak-Up):** prin formular securizat pe portalul intern CODATA.

CODATA garantează confidențialitatea completă și protecția identității avertizorilor, conform Directivei (UE) 2019/1937 privind protecția avertizorilor de integritate. Nicio persoană nu va fi sancționată pentru raportarea de bună credință a unei posibile abateri.

9. Sancțiuni

Încălcarea acestei politici atrage sancțiuni disciplinare, civile și, după caz, penale, inclusiv încetarea contractului de muncă sau colaborare.

CODATA aplică principiul „toleranță zero” și colaborează deplin cu autoritățile competente în investigarea oricărei fapte de corupție.

III. ANTI-BRIBERY AND ANTI-CORRUPTION POLICY

1. Purpose

The purpose of this policy is to prevent, identify, and eliminate any form of bribery, corruption, or unethical conduct within CODATA Software Solutions.

The company applies a **zero-tolerance policy** toward any action that could be construed as corruption, undue influence, or improper advantage.

This policy complements the principles set out in the **CODATA Code of Business Conduct and Ethics** and applies to all employees, partners, consultants, and subcontractors.

2. Definitions

- **Bribe:** any offer, promise, payment, gift, favor, or advantage intended to improperly influence a decision.
- **Corruption:** misuse of power or position for personal or collective gain, in exchange for favors, contracts, or confidential information.
- **Public Official:** any person holding a position in a government body, public agency, international organization, or state-owned enterprise.
- **Unauthorized Commission:** concealed or unjustified payment made to obtain a contract or business advantage.

3. General Principles

CODATA complies with all national and international anti-corruption laws, including:

- Romanian Law no. 78/2000 on preventing corruption;
- U.S. Foreign Corrupt Practices Act;
- U.K. Bribery Act;
- EU Directive 2017/1371 on protecting the financial interests of the EU.

All activities are conducted with integrity, transparency, and accountability toward clients, institutions, and partners.

4. Explicit Prohibitions

The following practices are strictly prohibited:

1. Offering, promising, or accepting money, gifts, or undue advantages.
2. Requesting or receiving donations or sponsorships intended to influence decisions.
3. Using intermediaries to disguise illegal payments.
4. Making facilitation payments to public officials, regardless of amount.
5. Political or charitable contributions that could be perceived as influencing decisions.
6. Hiring relatives of officials or partners without transparent evaluation.
7. Concealing or ignoring acts of corruption.

5. Gifts and Hospitality

CODATA allows only symbolic, reasonable, and transparent gestures of courtesy that:

- do not influence or appear to influence decisions;
- comply with business norms and internal rules;
- are pre-approved and recorded in the internal compliance registry.

Gifts, meals, or event invitations must remain modest and must be disclosed to management.

6. Relations with Public Officials and Institutions

In all interactions with national, EU or international, CODATA:

- follows formal and documented communication channels;
- records all meetings, contracts, and correspondence;
- prohibits any personal or financial advantage;
- applies full transparency to all publicly funded or co-financed projects.

7. Payments and Commissions

All CODATA payments must:

- be backed by a valid contract;
- include complete supporting documentation;
- be authorized in accordance with internal procedures.

Cash payments, personal account transfers, or unrecorded transactions are strictly forbidden.

8. Reporting and Whistleblower Protection

Any suspicion of bribery, illegal commissions, or corruption must be reported immediately via:

- **Dedicated email:** compliance@codata.ro
- **Internal Speak-Up Channel:** secure form via the CODATA portal.

CODATA ensures full confidentiality and whistleblower protection in accordance with **EU Directive 2019/1937**. No individual will suffer retaliation for reporting concerns in good faith.

9. Sanctions

Violation of this policy will result in disciplinary, civil, or criminal measures, including termination of employment or collaboration.

CODATA enforces a **zero-tolerance approach** and cooperates fully with competent authorities in the investigation of any corruption-related matter.

IV. POLITICA PRIVIND PREVENIREA ȘI COMBATEREA SPĂLĂRII BANILOR ȘI FINANȚĂRII TERORISMULUI

1. Scopul politicii

Această politică are ca obiectiv prevenirea utilizării activităților și produselor CODATA Software Solutions pentru scopuri ilegale, inclusiv spălarea banilor, finanțarea terorismului sau alte infracțiuni financiare.

CODATA adoptă un sistem intern de control și raportare în conformitate cu legislația română, europeană și internațională privind combaterea spălării banilor.

2. Cadrul legal

Politica se bazează pe următoarele reglementări:

- **Legea nr. 129/2019** pentru prevenirea și combaterea spălării banilor și finanțării terorismului;
- **Directivele UE (2015/849, 2018/843 și 2018/1673)** privind AML/CFT;
- **Regulamentele FATF (Financial Action Task Force)** privind standardele internaționale de conformitate;
- **Sancțiunile internaționale și embargourile impuse de UE, ONU și OFAC (SUA)**;
- **Normele ASF și BNR** privind raportarea tranzacțiilor suspecte și obligațiile de cunoaștere a clientelei (KYC).

3. Principii generale

CODATA respectă principiile fundamentale ale conformității financiare:

1. **Cunoașterea partenerilor de afaceri (KYC – Know Your Customer)**;
2. **Transparența fluxurilor financiare și a contractelor**;
3. **Interzicerea oricărei tranzacții cu entități aflate pe liste de sancțiuni internaționale**;
4. **Raportarea imediată a oricărei suspiciuni de tranzacții neregulate**;
5. **Păstrarea și arhivarea datelor conform legislației** (minim 5 ani).

4. Cunoașterea partenerilor (KYC / KYB)

Înainte de semnarea oricărui contract sau parteneriat, CODATA efectuează o **verificare completă a identității** și a istoricului entităților implicate. Procesul include:

- verificarea în registrul comerțului și în bazele de date oficiale;
- identificarea beneficiarilor reali și a structurii de acționariat;
- verificarea listelor de sancțiuni (OFAC, UE, ONU, UK HMT, NATO);
- analiza reputațională a entităților și persoanelor implicate;
- evaluarea riscului de conformitate și clasificarea partenerului în funcție de gradul de risc (scăzut, mediu, ridicat).

Nicio colaborare nu se aprobă fără finalizarea procedurii de due diligence.

5. Monitorizarea tranzacțiilor și raportarea suspiciunilor

CODATA monitorizează permanent fluxurile financiare, plățile și transferurile aferente contractelor, pentru a detecta:

- tranzacții neobișnuite ca valoare, frecvență sau structură;
- plăți prin intermediari fără justificare comercială;
- transferuri către jurisdicții cu risc ridicat (non-EU, offshore necooperante);
- plăți fragmentate sub pragurile de raportare.

Orice activitate suspectă se raportează imediat către:

- **Oficiul Național de Prevenire și Combatere a Spălării Banilor (ONPCSB)**;
- **Directorul de Conformitate CODATA** (responsabil intern AML/CFT).

6. Finanțarea terorismului și sancțiunile internaționale

CODATA interzice în mod absolut implicarea, directă sau indirectă, în activități care pot susține finanțarea terorismului, conform legislației naționale și listelor oficiale de sancțiuni. Compania nu va colabora și nu va efectua plăți către persoane sau entități:

- identificate pe listele UE, ONU, OFAC sau NATO ca susținătoare ale activităților teroriste;
- implicate în tranzacții cu arme, criptomonede nereglementate sau bunuri cu dublă utilizare fără licență;
- care refuză să furnizeze informațiile de identificare cerute prin lege.

7. Control intern și responsabilități

Pentru implementarea acestei politici, CODATA a desemnat un **Ofițer de Conformitate AML/CFT**, care:

- aplică procedurile KYC/KYB pentru toate entitățile contractante;
- monitorizează tranzacțiile și semnalează suspiciunile către ONPCSB;
- actualizează anual politicile și evaluările de risc AML/CFT;
- instruiește personalul asupra obligațiilor legale de raportare.

Toți angajații CODATA sunt obligați să colaboreze cu Ofițerul de Conformitate și să participe la programele de instruire obligatorie.

8. Păstrarea și protecția datelor

Documentele privind identificarea clienților, tranzacțiile și rapoartele AML sunt păstrate **minimum 5 ani** de la încetarea relației contractuale.

Datele se arhivează în medii securizate, cu acces restricționat, în conformitate cu **Regulamentul (UE) 2016/679 (GDPR)**și politicile interne de securitate cibernetică.

9. Sancțiuni și conformitate

Orice încălcare a prezentei politici constituie abatere gravă și poate conduce la măsuri disciplinare, civile sau penale. CODATA colaborează integral cu autoritățile competente și aplică principiul **"zero toleranță pentru neconformitate"**.

IV. ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING POLICY (AML/CFT)

1. Purpose

This policy aims to prevent the misuse of CODATA Software Solutions' operations, products, or services for illegal purposes such as money laundering, terrorist financing, or other financial crimes. CODATA implements internal controls and reporting mechanisms aligned with Romanian, EU, and international AML/CFT frameworks.

2. Legal Framework

This policy is based on:

- **Romanian Law no. 129/2019** on AML/CFT;
- **EU Directives 2015/849, 2018/843, and 2018/1673**;
- **FATF (Financial Action Task Force) Recommendations**;
- **EU, UN, and OFAC sanctions regulations**;
- **Local financial authority guidelines (ASF, BNR)**.

3. Core Principles

CODATA adheres to the following principles:

1. **Know Your Customer (KYC)** – mandatory identification of all clients and partners;
2. **Transparency** – all financial flows must be legitimate and traceable;
3. **Sanction Compliance** – prohibition of transactions with sanctioned entities;
4. **Suspicious Activity Reporting** – immediate escalation of irregular activities;
5. **Record Keeping** – secure retention of data for at least five years.

4. Know Your Customer (KYC / KYB)

Before any collaboration, CODATA performs full due diligence on all clients and partners, including:

- verification in official business registers;
- identification of beneficial owners and shareholding structure;
- screening against sanction lists (OFAC, EU, UN, UK HMT, NATO);
- reputational background checks;
- risk-based classification (low, medium, high).

No engagement proceeds without completion of the due diligence process.

5. Transaction Monitoring and Reporting

CODATA continuously monitors financial transactions to identify:

- unusual amounts, patterns, or frequency;
- intermediary payments lacking commercial justification;
- transfers to high-risk or non-cooperative jurisdictions;
- structured payments designed to evade thresholds.

Any suspicious activity must be reported to:

- **Romanian FIU (ONPCSB)**;
- **CODATA Compliance Director** (AML Officer).

6. Terrorist Financing and Sanctions

CODATA strictly prohibits any involvement, direct or indirect, in the financing of terrorism or dealings with sanctioned entities. The company will not conduct transactions with individuals or organizations:

- listed under EU, UN, OFAC, or NATO sanctions;
- engaged in arms trade, unregulated cryptocurrency operations, or dual-use goods without license;
- refusing to provide required identification or documentation.

7. Internal Controls and Responsibilities

A designated **AML/CFT Compliance Officer** is responsible for:

- applying KYC/KYB procedures to all partners;
- monitoring and reporting suspicious transactions;
- updating risk assessments and policies annually;
- delivering AML/CFT training to all staff.

All employees must cooperate with the Compliance Officer and comply with internal reporting requirements.

8. Record Keeping and Data Protection

All AML-related documents and transaction records are retained for **a minimum of five years** after the end of the business relationship. Data is securely archived in compliance with **GDPR (EU 2016/679)** and CODATA's cybersecurity policies.

9. Sanctions and Compliance

Any breach of this policy constitutes serious misconduct and may lead to disciplinary, civil, or criminal penalties.
CODATA enforces a **zero-tolerance policy** and fully cooperates with competent authorities in AML/CFT investigations.

V. POLITICA PRIVIND CONCURENȚA

1. Scopul politicii

Scopul acestei politici este de a asigura respectarea deplină a principiilor de concurență loială, transparență și integritate pe toate pieţele unde CODATA Software Solutions își desfășoară activitatea. CODATA se angajează să concureze prin inovație, calitate și competență, nu prin practici neloiale sau înțelegeri nepermise.

Respectarea regulilor de concurență este esențială pentru protejarea reputației companiei, a partenerilor și a clienților săi instituționali și privați.

2. Cadrul legal

Politica se bazează pe următoarele reglementări:

- **Legea concurenței nr. 21/1996 (România)**;
- **Articolele 101 și 102 din Tratatul privind funcționarea Uniunii Europene (TFUE)**;
- **Regulamentele Comisiei Europene privind practicile anticoncurențiale**;
- **Directivele privind achizițiile publice (UE 2014/24 și UE 2014/25)**;
- **Codurile etice aplicabile partenerilor instituționali (EIB, NATO, Comisia Europeană)**.

3. Principii generale

CODATA își fundamentează comportamentul comercial pe următoarele principii:

1. **Competiție liberă și echitabilă** – toate ofertele și parteneriatele se bazează pe merit, inovație și performanță.
2. **Transparență** – deciziile de afaceri sunt luate pe criterii obiective, fără înțelegeri ascunse.
3. **Respectarea confidențialității** – informațiile comerciale primite de la autorități sau clienți nu pot fi partajate cu competitori.
4. **Evitarea conflictelor de interese** – nicio persoană implicată în procesul de ofertare nu trebuie să aibă interese financiare sau personale în competiția respectivă.
5. **Conduită etică în licitații** – respectarea strictă a regulilor SICAP, PNRR, EIB, NATO și a principiilor „best value for money”.

4. Practici interzise

CODATA interzice în mod expres orice acțiune care ar putea fi interpretată drept practică anticoncurențială, inclusiv:

- înțelegeri privind fixarea prețurilor, împărțirea piețelor, clienților sau contractelor;
- schimb de informații sensibile cu competitori;
- acțiuni coordonate care limitează competiția în licitații (bid-rigging, cover bidding, subcontractări fictive);
- restricționarea accesului altor operatori economici la piețe sau resurse;
- abuz de poziție dominantă, exploatarea clienților prin prețuri nejustificat de mari sau condiții inechitabile;
- orice formă de înțelegere tacită între competitori pentru excluderea unui participant.

5. Conduita în procesul de achiziție publică

În cadrul participării la licitații publice, CODATA respectă următoarele reguli:

- pregătirea ofertelor în mod independent, fără consultarea concurenților;
- interdicția de a comunica altor participanți conținutul ofertelor tehnice sau financiare;
- utilizarea doar a informațiilor publice sau oficiale puse la dispoziție de autorități;

- evitarea contactelor neautorizate cu reprezentanții achizitorului pe durata procedurii;
- declararea completă a subcontractanților și a partenerilor, conform cerințelor legale;
- păstrarea integrității și confidențialității datelor de ofertare.

Orice abatere de la aceste reguli poate conduce la excluderea din licitații și la sancțiuni legale.

6. Relațiile cu competiția și partenerii

CODATA promovează **colaborarea etică** și **parteneriatele strategice transparente**, bazate pe:

- respect reciproc și competiție loială;
- schimb de informații limitat la aspecte tehnice publice;
- interdicția oricăror acorduri privind prețurile, condițiile comerciale sau împărțirea contractelor;
- consultări doar în cadrul consorțiilor sau joint venture-urilor aprobate prin contracte legale și transparente.

7. Raportare și conformitate

Orice angajat sau partener care suspectează o practică anticoncurențială trebuie să raporteze imediat incidentul la: **compliance@codata.ro**

CODATA asigură confidențialitatea și protecția completă a persoanelor care semnalează astfel de cazuri. Departamentul de Conformitate investighează toate sesizările și, dacă este cazul, cooperează cu autoritățile de concurență naționale și europene.

8. Consecințe

Încălcarea acestei politici poate duce la:

- sancțiuni disciplinare sau concediere;
- excluderea companiei din proceduri de achiziție publică;
- amenzi semnificative impuse de autoritățile de concurență;
- pierderea statutului de partener certificat.

CODATA aplică principiul **„toleranță zero față de comportamentul anticoncurențial”**.

V. COMPETITION POLICY

1. Purpose

The purpose of this policy is to ensure full compliance with fair competition, transparency, and integrity across all markets where CODATA Software Solutions operates. CODATA competes through innovation, quality, and performance never through collusion or unfair practices.

Compliance with competition laws protects CODATA’s reputation and builds trust among clients, public authorities, and partners.

2. Legal Framework

This policy is based on:

- **Romanian Competition Law no. 21/1996**;
- **Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU)**;
- **European Commission regulations on anti-competitive behavior**;
- **EU Public Procurement Directives (2014/24/EU and 2014/25/EU)**;
- **Ethical codes of institutional partners.**

3. Core Principles

CODATA's conduct is guided by the following principles:

1. **Free and fair competition** based on innovation and competence;
2. **Transparency** in all business decisions;
3. **Confidentiality** of all proprietary or bid-related information;
4. **Conflict of interest avoidance** for all employees involved in tenders;
5. **Ethical procurement conduct** in compliance with SICAP, PNRR, and international standards.

4. Prohibited Practices

The following behaviors are strictly forbidden:

- price-fixing or market-sharing agreements;
- exchange of confidential information with competitors;
- bid-rigging or collusive tendering;
- restricting access to markets or clients;
- abuse of dominant position;
- implicit or explicit agreements to exclude competitors.

5. Conduct in Public Procurement

When participating in public tenders, CODATA must:

- prepare bids independently;
- avoid sharing technical or financial details with competitors;
- use only publicly available information;
- refrain from unauthorized contact with contracting authorities;
- disclose subcontractors and partners transparently;
- maintain confidentiality and integrity of tender documents.

Violations may result in disqualification and legal penalties.

6. Relations with Competitors and Partners

CODATA encourages **ethical collaboration** and **transparent strategic alliances**, based on:

- mutual respect and fair competition;
- limited information exchange restricted to public or technical aspects;
- prohibition of price or market allocation agreements;
- partnerships only through legally binding and transparent contracts.

7. Reporting and Compliance

Any suspected anti-competitive conduct must be reported to **compliance@codata.ro**

CODATA guarantees confidentiality and protection for whistleblowers. The Compliance Department investigates all reports and cooperates with competition authorities when required.

8. Consequences

Violations of this policy may result in:

- disciplinary action or termination;
- exclusion from procurement processes;
- financial penalties imposed by competition authorities;
- revocation of partner certifications.

CODATA enforces a **zero-tolerance policy toward anti-competitive behavior**.

VI. POLITICA PRIVIND CONFIDENȚIALITATEA ȘI PROTECȚIA INFORMAȚIILOR

1. Scopul politicii

Această politică are scopul de a proteja informațiile confidențiale, datele personale și secretele comerciale ale CODATA Software Solutions, ale clienților și partenerilor săi. CODATA tratează securitatea informațională ca pe o prioritate strategică, asigurând confidențialitatea, integritatea și disponibilitatea tuturor datelor procesate în activitățile sale.

Prin această politică, compania garantează conformitatea cu legislația privind protecția datelor, normele internaționale de securitate cibernetică și obligațiile contractuale asumate în relațiile cu terți.

2. Domeniul de aplicare

Politica se aplică tuturor:

- angajaților CODATA, indiferent de poziție;
- consultanților, subcontractorilor și colaboratorilor;
- partenerilor care au acces la date, infrastructură IT sau sisteme de producție CODATA;
- proiectelor desfășurate pentru instituții publice, clienți privați sau organizații internaționale.

3. Tipuri de informații protejate

Sunt considerate **informații confidențiale**:

- datele personale ale angajaților, clienților și partenerilor;
- documente comerciale, tehnice, financiare sau juridice;
- informații privind arhitecturi IT, infrastructuri cloud, baze de date, soluții AI și algoritmi proprietari;
- cod sursă, modele de inteligență artificială, parametri de antrenare și rezultate de testare;
- rapoarte interne, planuri de proiect, corespondență și documente de licitație;
- orice informație clasificată „internă", „confidențială", „restricționată" sau „securizată" în sistemele CODATA.

4. Principii fundamentale

CODATA respectă următoarele principii:

1. **Confidențialitate** – accesul la informații se acordă doar persoanelor autorizate.
2. **Integritate** – datele trebuie protejate împotriva modificării, pierderii sau distrugerii neautorizate.
3. **Disponibilitate** – informațiile trebuie să fie accesibile doar în limitele definite de politici și contracte.
4. **Minimizarea datelor** – se colectează doar informațiile strict necesare scopului procesării.
5. **Responsabilitate** – fiecare utilizator este răspunzător pentru modul în care gestionează datele.
6. **Securitate prin design** – toate soluțiile IT dezvoltate de CODATA integrează protecția datelor încă din faza de proiectare.

5. Protecția datelor personale (GDPR)

CODATA este operator de date conform **Regulamentului (UE) 2016/679 (GDPR)** și aplică următoarele măsuri:

- desemnarea unui **Responsabil cu protecția datelor (DPO)**;
- respectarea drepturilor persoanelor vizate (informare, acces, rectificare, ștergere, opoziție, portabilitate);
- evaluări de impact (DPIA) pentru proiecte complexe sau care implică prelucrarea datelor sensibile;
- acorduri de confidențialitate (NDA) cu toți angajații și partenerii;
- criptarea comunicațiilor și a bazelor de date;
- audituri periodice interne și externe privind conformitatea GDPR.

Datele personale nu sunt transferate către state terțe fără garanții adecvate și nici partajate cu terți fără bază legală.

6. Securitate cibernetică (ISO 27001 / NIS2)

CODATA menține un **Sistem de Management al Securității Informației (ISMS)** conform ISO 27001 și implementat pe următoarele direcții:

- control al accesului bazat pe rol (RBAC);
- autentificare multifactor (MFA) pentru toți utilizatorii;
- criptare end-to-end pentru comunicații și date stocate;
- politici de backup, restaurare și continuitate operațională (BCP / DRP);
- monitorizare constantă a infrastructurii și alertare automată pentru incidente de securitate;
- raportarea incidentelor în maximum 72 de ore, conform legislației NIS2.

Orice incident de securitate informatică este documentat și investigat de echipa tehnică împreună cu Ofițerul de Conformitate.

7. Confidențialitatea în proiecte și licitații

În cadrul proiectelor publice și al licitațiilor, CODATA:

- tratează toate documentele primite ca **informații confidențiale**;
- nu divulgă detalii tehnice, financiare sau juridice către terți;
- respectă prevederile clauzelor de confidențialitate din contracte;
- asigură protecția datelor prin servere securizate, logare detaliată și audit tehnic permanent;
- implementează controale TEMPEST și criptare hardware pentru proiectele NATO sau clasificate.

8. Responsabilități

Responsabilitatea pentru protecția informațiilor este comună:

- **Consiliul de Administrație** definește politicile generale;
- **Ofițerul de Conformitate și DPO-ul** monitorizează respectarea reglementărilor;
- **Departamentul IT & Security** asigură implementarea măsurilor tehnice;
- **Toți angajații și partenerii** au obligația de a proteja informațiile accesate și de a raporta imediat orice incident la **security@codata.ro** sau **compliance@codata.ro**.

9. Sancțiuni

Încălcarea politicii de confidențialitate atrage măsuri disciplinare și, după caz, răspundere civilă sau penală.
CODATA aplică principiul **„securitate fără compromisuri”** și colaborează permanent cu autoritățile de reglementare și instituțiile partenere.

VI. CONFIDENTIALITY AND INFORMATION PROTECTION POLICY

1. Purpose

This policy aims to protect the confidential information, personal data, and trade secrets of CODATA Software Solutions, its clients, and partners.

CODATA treats information security as a strategic priority, ensuring confidentiality, integrity, and availability of all data processed in its operations.

2. Scope

The policy applies to:

- all CODATA employees;
- consultants, subcontractors, and collaborators;
- partners with access to data, IT infrastructure, or CODATA systems;
- all public or private sector projects, including EU and NATO programs.

3. Protected Information

Confidential information includes:

- personal data of employees, clients, and partners;
- commercial, technical, financial, or legal documents;
- IT architectures, cloud infrastructures, AI models, databases, and algorithms;
- source code, training datasets, and AI testing outputs;
- internal reports, correspondence, and bid documentation;
- any information labeled “internal,” “confidential,” or “restricted.”

4. Core Principles

CODATA’s information management follows six key principles:

1. **Confidentiality** – access granted only to authorized persons.
2. **Integrity** – data protected from unauthorized modification or loss.
3. **Availability** – access permitted within contractual and policy limits.
4. **Data Minimization** – collect only what is strictly necessary.
5. **Accountability** – all users are responsible for data handling.
6. **Security by Design** – all IT solutions embed privacy and security from inception.

5. Personal Data Protection (GDPR)

CODATA complies with **EU Regulation 2016/679 (GDPR)** by:

- appointing a **Data Protection Officer (DPO)**;
- upholding individual rights (access, rectification, deletion, objection, portability);
- conducting Data Protection Impact Assessments (DPIA) where required;
- enforcing NDAs with all staff and partners;
- encrypting all communications and databases;
- performing regular compliance audits.

No personal data is transferred outside the EU without adequate safeguards or shared with third parties without legal basis.

6. Cybersecurity (ISO 27001 / NIS2)

CODATA operates an **Information Security Management System (ISMS)** aligned with ISO 27001, including:

- role-based access control (RBAC);
- multi-factor authentication (MFA);

- end-to-end encryption;
- backup and disaster recovery policies (BCP/DRP);
- continuous infrastructure monitoring;
- 72-hour incident reporting under NIS2.

All cybersecurity incidents are logged, analyzed, and remediated by the IT Security and Compliance teams.

7. Confidentiality in Projects and Tenders

In all tenders and public projects, CODATA:

- treats all received documents as confidential;
- never discloses technical or financial data to unauthorized parties;
- respects NDAs and contractual confidentiality clauses;
- protects data via secure servers, detailed logging, and periodic audits;
- implements TEMPEST controls and hardware encryption for classified NATO projects.

8. Responsibilities

Responsibility for information protection lies with:

- **Board of Directors** – defines policy and oversight;
- **Compliance Officer & DPO** – ensure regulatory alignment;
- **IT & Security Department** – enforce technical safeguards;
- **All employees and partners** – must protect accessed data and report any incident to **security@codata.ro** or **compliance@codata.ro**.

9. Sanctions

Any breach of this policy may result in disciplinary, civil, or criminal action. CODATA enforces the principle of **"security without compromise"** and cooperates fully with regulatory bodies and institutional partners.

VII. POLITICA DE PREVENIRE A FRAUDEI INTERNE

1. Scopul politicii

Scopul acestei politici este de a preveni, detecta și combate orice formă de fraudă, abuz sau utilizare neautorizată a resurselor companiei. CODATA Software Solutions adoptă o abordare de **toleranță zero față de frauda internă**, indiferent de valoare, poziție ierarhică sau intenție.

Politica definește cadrul de guvernanță, responsabilitățile și procedurile interne pentru menținerea unui mediu de lucru etic, transparent și sigur.

2. Definiția fraudei

Prin „fraudă” se înțelege orice acțiune sau omisiune intenționată, comisă de un angajat, colaborator, consultant sau partener, având scopul de a obține un beneficiu necuvenit sau de a prejudicia compania, clienții sau instituțiile partenere.

Exemple de fraudă includ:

- falsificarea sau manipularea documentelor contabile, tehnice sau de proiect;
- utilizarea neautorizată a sistemelor informatice sau accesarea datelor fără drept;
- deturnarea de fonduri, comisioane sau resurse materiale;
- conflict de interese nedeclarat;
- favorizarea anumitor furnizori, subcontractori sau parteneri în schimbul unor avantaje;
- utilizarea informațiilor confidențiale în scop personal sau extern;
- raportarea falsă a activităților, livrabilelor sau costurilor în proiecte.

3. Principii de prevenire

Pentru a reduce riscul de fraudă internă, CODATA aplică următoarele principii:

1. **Separarea atribuțiilor** – nicio persoană nu deține control complet asupra unei operațiuni financiare sau tehnice.
2. **Trasabilitate completă** – toate procesele sunt documentate și auditate periodic.
3. **Control dublu (four-eyes principle)** – aprobările critice se efectuează de minimum două persoane independente.
4. **Audit intern și extern permanent** – verificări tehnice, contabile și de conformitate la nivel de proiect și organizație.
5. **Monitorizare digitală** – sistemele IT includ logare automată, control de acces și alerte pentru activități neautorizate.
6. **Etică organizațională** – instruirea periodică a personalului privind riscurile și consecințele fraudei.

4. Zone de risc

Frauda internă poate apărea în următoarele zone:

- achiziții și relații cu furnizorii;
- gestiunea contractelor și raportarea livrabilelor;
- deconturi, plăți, facturare și contabilitate;
- accesul la infrastructuri IT, servere și baze de date;
- manipularea datelor sau a documentelor digitale (scanare, OCR, arhivare);
- proiecte finanțate din fonduri publice sau europene.

Fiecare departament este obligat să evalueze anual riscurile de fraudă și să implementeze măsuri corective.

5. Mecanisme de control și detectare

CODATA implementează un sistem integrat de prevenire și detectare a fraudei, care include:

- **sistem ERP integrat** pentru controlul documentelor și al fluxurilor financiare;
- **monitorizare IT automată** pentru activități neobișnuite sau acces neautorizat;
- **audit intern trimestrial**, coordonat de Directorul Financiar și Ofițerul de Conformitate;
- **verificarea furnizorilor** prin proceduri KYC/KYB;
- **canal de raportare anonimă (whistleblowing)** prin platforma internă „Speak-Up”;

- **revizuire post-incident** pentru a identifica cauzele și a preveni recurența.

6. Raportare și protecția avertizorilor

Orice suspiciune de fraudă trebuie raportată imediat prin:

- **email:** compliance@codata.ro
- **platforma internă „Speak-Up”** (acces securizat)
- **linie de etică** disponibilă 24/7 pentru raportări anonime.

CODATA asigură confidențialitatea totală și protejează avertizorii de orice formă de represalii, conform Directivei (UE) 2019/1937 privind protecția avertizorilor de integritate.

7. Investigații interne

După primirea unei sesizări:

1. Ofițerul de Conformitate inițiază o **analiză preliminară** pentru validarea informației.
2. Dacă există indicii rezonabile, se formează o **echipă de investigație internă**, cu participarea departamentelor juridic, financiar și IT.
3. Toate investigațiile se desfășoară confidențial, documentat și imparțial.
4. Rezultatele sunt prezentate Consiliului de Administrație, care decide măsurile administrative și legale.

Dacă este cazul, CODATA cooperează deplin cu organele de urmărire penală și autoritățile competente.

8. Sancțiuni

Orice act de fraudă confirmat atrage:

- sancțiuni disciplinare, inclusiv concediere imediată;
- recuperarea prejudiciului material;
- sesizarea organelor judiciare;
- interdicția permanentă de colaborare cu CODATA.

CODATA aplică principiul **„Integritate absolută. Toleranță zero față de fraudă”**.

VII. INTERNAL FRAUD PREVENTION POLICY

1. Purpose

The purpose of this policy is to prevent, detect, and combat any form of fraud, abuse, or unauthorized use of company resources. CODATA Software Solutions maintains a **zero-tolerance stance toward internal fraud**, regardless of position or intent.

The policy defines governance, responsibilities, and procedures to ensure an ethical, transparent, and secure work environment.

2. Definition of Fraud

Fraud refers to any intentional act or omission by an employee, collaborator, or partner aimed at gaining an undue advantage or causing harm to the company, clients, or institutions.

Examples include:

- falsification or manipulation of accounting, technical, or project documents;
- unauthorized access to IT systems or confidential data;
- misappropriation of funds, commissions, or assets;
- undisclosed conflicts of interest;
- favoritism in supplier or partner selection;
- misuse of confidential information for personal or external benefit;
- falsified reporting of project activities or deliverables.

3. Prevention Principles

CODATA enforces the following principles to reduce fraud risk:

1. **Segregation of Duties** – no individual has total control over a financial or operational process.
2. **Full Traceability** – all actions are documented and subject to audit.
3. **Four-Eyes Principle** – critical approvals require two independent authorizations.
4. **Regular Audits** – internal and external verification of technical, financial, and compliance processes.
5. **Digital Monitoring** – IT systems include automated logging and anomaly detection.
6. **Ethical Awareness** – mandatory staff training on fraud prevention and reporting.

4. Areas of Risk

Potential areas for internal fraud include:

- procurement and supplier relations;
- contract and deliverable management;
- invoicing and accounting;
- access to IT systems and databases;
- manipulation of digital archives or document processing (OCR, digitization);
- publicly or EU-funded projects.

Each department must perform an annual fraud risk assessment and implement corrective measures.

5. Control and Detection Mechanisms

CODATA maintains an integrated fraud prevention system including:

- **ERP workflow controls** for financial transactions;
- **IT activity monitoring and alerting**;
- **quarterly internal audits** led by Finance and Compliance;
- **supplier due diligence** (KYC/KYB);
- **anonymous reporting via Speak-Up channel**;
- **post-incident review and mitigation planning**.

6. Reporting and Whistleblower Protection

All suspicions of fraud must be reported immediately to:

- **Email:** compliance@codata.ro
- **Internal Speak-Up Platform** (secure access)
- **Ethics hotline** (available 24/7).

CODATA guarantees full confidentiality and protects whistleblowers from retaliation in compliance with **EU Directive 2019/1937**.

7. Internal Investigations

Upon receiving a report:

1. The Compliance Officer performs a preliminary review.
2. If evidence is found, an **Investigation Team** is formed (Legal, Finance, IT).
3. Investigations are conducted confidentially and objectively.
4. Findings are presented to the **Board of Directors**, which decides on disciplinary and legal action.

CODATA fully cooperates with judicial and regulatory authorities when required.

8. Sanctions

Confirmed fraud results in:

- disciplinary measures, including termination;
- recovery of damages;
- criminal complaint to authorities;
- permanent exclusion from future collaborations.

CODATA enforces the principle **"Absolute Integrity. Zero Tolerance for Fraud."**

VIII. POLITICA DE CONDUITĂ ȘI COMPORTAMENT ÎN CODATA

1. Scopul politicii

Această politică stabilește standardele de comportament și conduită profesională pentru toți angajații, colaboratorii și partenerii CODATA Software Solutions. Obiectivul este crearea unui mediu de lucru bazat pe **respect, integritate, responsabilitate și performanță**, în care fiecare persoană contribuie la reputația și succesul organizației.

2. Principii fundamentale de conduită

CODATA promovează o cultură a comportamentului etic și profesional, bazată pe următoarele principii:

1. **Integritate** – acționează corect, fără compromisuri morale sau legale.
2. **Respect** – tratează colegii, clienții și partenerii cu politețe, fără discriminare sau abuz.
3. **Responsabilitate** – asumă-ți deciziile și consecințele lor.
4. **Transparență** – comunică deschis, corect și complet.

5. **Profesionalism** – oferă soluții de calitate, respectă termenele și standardele stabilite.
6. **Colaborare** – lucrează în echipă, împărtășește cunoștințe și sprijină colegii.
7. **Confidențialitate** – păstrează discreția privind informațiile interne și ale clienților.

3. Relațiile profesionale

În cadrul CODATA:

- relațiile de muncă se bazează pe respect reciproc și colaborare deschisă;
- se interzic orice forme de hărțuire, intimidare, discriminare sau abuz de autoritate;
- fiecare angajat trebuie să mențină un comportament civilizat și constructiv, indiferent de poziție;
- conducerea are obligația de a asculta și de a rezolva problemele semnalate în mod obiectiv.

Comunicarea internă trebuie să fie clară, profesionistă și orientată spre soluții, evitând tonul agresiv sau nepotrivit.

4. Utilizarea resurselor companiei

Toate resursele CODATA echipamente IT, software, servere, conturi de e-mail, vehicule, telefoane sau spații trebuie utilizate exclusiv în scop profesional. Este interzisă:

- utilizarea infrastructurii IT pentru activități personale, politice sau ilegale;
- accesarea, copierea sau transmiterea neautorizată a datelor;
- instalarea de aplicații neautorizate;
- folosirea identității companiei în scop personal (rețele sociale, e-mail, corespondență privată).

Sistemele IT sunt monitorizate pentru a asigura protecția datelor și respectarea politicilor interne.

5. Conflicte de interese

Angajații și colaboratorii CODATA trebuie să evite orice situație în care interesele personale pot afecta obiectivitatea profesională. Exemple:

- participarea la decizii care implică rude, prieteni sau companii afiliate;
- implicarea în activități comerciale concurente;
- acceptarea de beneficii care pot influența decizii profesionale.

Toate potențialele conflicte de interese trebuie raportate imediat la **compliance@codata.ro**

6. Comportament în mediul extern

În relația cu clienții, autoritățile, partenerii și presa, fiecare reprezentant CODATA trebuie să:

- acționeze cu profesionalism, imparțialitate și discreție;
- evite declarațiile publice fără mandatul conducerii;
- mențină imaginea de seriozitate și competență a companiei;
- respecte codurile etice ale partenerilor instituționali.

Orice comunicare externă oficială trebuie aprobată de Departamentul de Comunicare.

7. Mediu de lucru și diversitate

CODATA susține un mediu de lucru sigur, incluziv și echilibrat, în care:

- se promovează egalitatea de șanse și diversitatea;
- se interzice orice formă de discriminare bazată pe gen, vârstă, religie, orientare, origine sau opinie;
- se încurajează dezvoltarea profesională continuă și inițiativa personală;
- se oferă suport pentru echilibrul între viața profesională și cea personală.

8. Mecanisme de raportare

Orice abatere de la politica de conduită poate fi raportată confidențial prin:

- **email:** compliance@codata.ro
- **platforma internă „Speak-Up”** (anonimă și securizată).

CODATA investighează toate sesizările cu obiectivitate și protejează angajații care raportează de bună credință.

9. Sancțiuni

Încălcarea politicii de conduită poate atrage sancțiuni disciplinare, până la încetarea contractului de muncă. CODATA consideră conduita etică o condiție fundamentală a apartenenței la organizație.

VIII. CODE OF CONDUCT AND BEHAVIOR POLICY

1. Purpose

This policy defines the behavioral and ethical standards expected from all CODATA Software Solutions employees, collaborators, and partners. Its goal is to foster a workplace culture based on **respect, integrity, accountability, and performance**.

2. Core Conduct Principles

CODATA promotes a professional and ethical environment guided by:

1. **Integrity** – act lawfully and ethically in every situation.
2. **Respect** – treat others with fairness and dignity.
3. **Accountability** – take ownership of your actions and outcomes.
4. **Transparency** – communicate honestly and clearly.
5. **Professionalism** – meet commitments with quality and precision.
6. **Collaboration** – support teamwork and mutual growth.

7. **Confidentiality** – safeguard internal and client information.

3. Professional Relationships

At CODATA:

- interactions are based on mutual respect and cooperation;
- harassment, intimidation, and discrimination are strictly forbidden;
- all employees must maintain a constructive and courteous tone;
- management must listen and act impartially when resolving concerns.

Internal communication should be professional and solution-oriented.

4. Use of Company Resources

All company assets IT equipment, software, servers, email accounts, vehicles, and offices must be used **only for legitimate business purposes**. The following are prohibited:

- using infrastructure for personal, political, or illegal purposes;
- unauthorized access or data transmission;
- installation of unapproved software;
- using the company's name or identity for personal activities.

All systems are monitored to ensure compliance and security.

5. Conflicts of Interest

Employees and partners must avoid any situation where personal interests conflict with professional duties.
Examples include:

- decision-making involving relatives or affiliated entities;
- participation in competing businesses;
- accepting benefits that could influence professional judgment.

Potential conflicts must be reported immediately to **compliance@codata.ro**

6. External Conduct

When representing CODATA to clients, authorities, or media, all personnel must:

- act professionally and impartially;
- refrain from public statements without authorization;
- maintain the company's image of reliability and expertise;
- adhere to partners' ethical standards.

Official communications require approval from the Communication Department.

7. Workplace and Diversity

CODATA fosters a safe, inclusive, and equitable work environment that:

- promotes equal opportunity and diversity;
- prohibits all forms of discrimination;
- supports professional development and work-life balance;
- values initiative, learning, and mutual respect.

8. Reporting Mechanisms

Any breach of this policy may be reported confidentially through:

- **Email:** compliance@codata.ro
- **Speak-Up Platform:** anonymous and secure.

All reports are investigated objectively, and whistleblowers are fully protected.

9. Sanctions

Violations of this Code may result in disciplinary action, up to and including termination. CODATA considers ethical conduct a core requirement of belonging to the organization.

IX. POLITICA PRIVIND PROTECȚIA MEDIULUI ȘI SUSTENABILITATEA

1. Scopul politicii

Scopul acestei politici este de a integra principiile de protecție a mediului și sustenabilitate în toate activitățile CODATA Software Solutions. CODATA recunoaște responsabilitatea sa față de mediu și se angajează să reducă impactul ecologic al operațiunilor sale prin practici eficiente, inovatoare și responsabile.

2. Obiective generale

CODATA urmărește:

1. reducerea consumului de energie și resurse;
2. gestionarea responsabilă a deșeurilor și reciclarea materialelor;
3. promovarea achizițiilor verzi și a echipamentelor eficiente energetic;
4. reducerea amprentei de carbon în activitățile zilnice;
5. digitalizarea proceselor pentru eliminarea hârtiei;
6. conștientizarea și implicarea angajaților în acțiuni de mediu.

3. Cadrul legal și standarde

Politica se bazează pe:

- **ISO 14001:2015 – Sistem de Management de Mediu**;
- **Pactul Ecologic European (EU Green Deal)**;
- **Regulamentele UE privind gestionarea deșeurilor electronice (WEEE)**;
- **Legea nr. 211/2011 privind regimul deșeurilor**;
- **Reglementările privind achizițiile durabile (Green Public Procurement – GPP)**.

4. Principii de acțiune

CODATA aplică următoarele principii:

1. **Prevenție** – reducerea de la sursă a poluării și a risipei;
2. **Eficiență energetică** – optimizarea consumului de energie în centrele de date, birouri și echipamente IT;
3. **Digitalizare verde** – promovarea soluțiilor cloud și paperless în proiectele publice și private;
4. **Reciclare și reutilizare** – colectarea selectivă și reciclarea echipamentelor IT, hârtiei și ambalajelor;
5. **Achiziții verzi** – selectarea furnizorilor care respectă criterii de sustenabilitate și standarde de mediu;
6. **Compensare și neutralitate** – reducerea emisiilor și sprijinirea proiectelor de compensare a carbonului.

5. Gestionarea resurselor

CODATA optimizează utilizarea resurselor prin:

- instalarea de echipamente cu consum redus de energie;
- utilizarea infrastructurii cloud în locul centrelor de date locale, acolo unde este posibil;
- automatizarea iluminatului, temperaturii și consumului în birouri;
- implementarea unui sistem de monitorizare a consumului de electricitate și apă;
- eliminarea completă a imprimării neesențiale prin semnătură digitală și fluxuri electronice.

6. Deșeuri și reciclare

CODATA aplică principiul „Reduce – Reuse – Recycle”. Toate echipamentele IT scoase din uz sunt predate partenerilor autorizați pentru reciclare, iar bateriile, cartușele și deșeurile electronice sunt colectate separat. Materialele reciclabile (hârtie, plastic, sticlă) sunt colectate diferențiat în toate birourile.

7. Achiziții verzi

La selecția furnizorilor, CODATA ia în considerare:

- certificările de mediu (ISO 14001, Energy Star, RoHS);
- utilizarea ambalajelor reciclabile și reducerea plasticului;
- performanța energetică a produselor;

- conformitatea cu directivele UE privind reducerea emisiilor.

CODATA preferă partenerii care aplică politici de sustenabilitate similare și demonstrează practici de mediu responsabile.

8. Conștientizare și responsabilitate

Toți angajații CODATA sunt instruiți periodic privind:

- reducerea consumului de resurse;
- reciclarea corectă;
- utilizarea sustenabilă a echipamentelor;
- impactul activităților IT asupra mediului.

Conducerea susține inițiativele individuale sau de echipă care contribuie la protecția mediului.

9. Monitorizare și îmbunătățire continuă

CODATA monitorizează anual performanța de mediu prin:

- audituri interne;
- indicatori de eficiență energetică și deșeuri reciclate;
- raportări către autorități și parteneri instituționali.

Rezultatele sunt analizate și folosite pentru îmbunătățirea continuă a sistemului de management de mediu.

IX. ENVIRONMENTAL PROTECTION AND SUSTAINABILITY POLICY

1. Purpose

This policy integrates environmental protection and sustainability principles into all CODATA Software Solutions operations. CODATA acknowledges its environmental responsibility and is committed to minimizing ecological impact through efficient and responsible practices.

2. Objectives

CODATA aims to:

1. reduce energy and resource consumption;
2. manage waste responsibly and promote recycling;
3. implement green procurement and energy-efficient technologies;
4. lower carbon footprint across all operations;
5. promote paperless digital transformation;
6. raise environmental awareness among employees.

3. Legal Framework and Standards

This policy is aligned with:

- **ISO 14001:2015 Environmental Management System**;
- **EU Green Deal**;
- **EU Waste Electrical and Electronic Equipment (WEEE) regulations**;
- **Romanian Law no. 211/2011 on waste management**;
- **EU Green Public Procurement (GPP) directives**.

4. Action Principles

CODATA follows key principles:

1. **Prevention** – minimize waste and pollution at source;
2. **Energy Efficiency** – optimize energy use in offices and data centers;
3. **Green Digitalization** – promote cloud and paperless solutions;
4. **Recycling and Reuse** – ensure proper segregation and recycling of materials;
5. **Green Procurement** – select eco-conscious suppliers;
6. **Carbon Neutrality** – reduce emissions and support offset initiatives.

5. Resource Management

CODATA enhances resource efficiency through:

- use of low-consumption equipment;
- migration to cloud infrastructure;
- automated lighting and temperature control;
- monitoring systems for energy and water use;
- electronic workflows to eliminate unnecessary printing.

6. Waste and Recycling

CODATA applies the "Reduce – Reuse – Recycle" principle. All obsolete IT equipment is recycled by certified partners, and office waste is segregated for proper disposal. Recyclable materials (paper, plastic, glass) are collected separately at all company sites.

7. Green Procurement

When selecting suppliers, CODATA evaluates:

- environmental certifications (ISO 14001, Energy Star, RoHS);
- recyclable packaging;
- product energy efficiency;
- compliance with EU emission standards.

Preference is given to partners demonstrating sustainable practices.

8. Awareness and Responsibility

All employees receive regular training on:

- resource optimization;
- waste reduction and recycling;
- sustainable equipment use;
- environmental impact of IT operations.

Management encourages and supports employee-led environmental initiatives.

9. Monitoring and Continuous Improvement

CODATA monitors its environmental performance annually through:

- internal audits;
- sustainability indicators (energy, waste, CO_2 reduction);
- reporting to authorities and institutional partners.

Results guide ongoing improvements to the environmental management system.

X. POLITICA PRIVIND SECURITATEA INFORMATICĂ ȘI PROTECȚIA INFRASTRUCTURII DIGITALE

1. Scopul politicii

Scopul acestei politici este de a proteja infrastructura informatică, sistemele digitale, datele și serviciile CODATA Software Solutions împotriva accesului neautorizat, pierderii, coruperii sau compromiterii. CODATA consideră securitatea informatică o **responsabilitate strategică** și o condiție esențială pentru desfășurarea activităților sale în siguranță, conform celor mai înalte standarde internaționale.

2. Domeniul de aplicare

Politica se aplică tuturor:

- sistemelor IT utilizate în cadrul companiei (servere, aplicații, cloud, infrastructuri de rețea);
- angajaților, colaboratorilor, subcontractorilor și partenerilor care accesează aceste sisteme;
- proiectelor naționale și internaționale gestionate de CODATA, inclusiv cele clasificate sau finanțate de instituții publice.

3. Obiective generale

CODATA urmărește:

1. protejarea informațiilor și infrastructurii digitale;

2. asigurarea confidențialității, integrității și disponibilității datelor (model CIA);
3. prevenirea incidentelor de securitate cibernetică;
4. reacția rapidă și coordonată în cazul atacurilor;
5. conformitatea cu reglementările legale și contractuale privind protecția datelor și securitatea IT.

4. Cadrul legal și standarde aplicabile

Politica respectă următoarele standarde și reglementări:

- **ISO/IEC 27001:2022 – Managementul Securității Informației**;
- **Directiva (UE) 2022/2555 – NIS2**;
- **Regulamentul (UE) 2016/679 – GDPR**;
- **CIS Critical Security Controls (v8)**;
- **STANAG 4774/4778 (NATO) – Data Protection & Secure Exchange**;
- **Legislația națională privind securitatea cibernetică și protecția infrastructurilor critice**.

5. Principii de securitate

CODATA aplică următoarele principii de bază:

1. **Minim drepturi, maxim control** – fiecare utilizator are acces doar la resursele strict necesare.
2. **Zero Trust Architecture** – niciun dispozitiv, cont sau rețea nu este implicit de încredere.
3. **Segregarea rețelelor** – separarea mediilor de producție, testare și administrare.
4. **Autentificare multifactor (MFA)** pentru toate conturile privilegiate.
5. **Criptare completă (end-to-end)** pentru datele stocate și transmise.
6. **Monitorizare și audit permanent** – toate activitățile IT sunt logate și analizate.
7. **Actualizare continuă (patch management)** – toate sistemele sunt menținute la zi.
8. **Backup și recuperare** – existența unui plan de continuitate (BCP/DRP) testat anual.

6. Clasificarea și protecția datelor

CODATA clasifică informațiile digitale în patru niveluri:

1. **Publice** – pot fi distribuite liber.
2. **Interne** – destinate exclusiv personalului CODATA.
3. **Confidențiale** – restricționate la persoane autorizate.
4. **Critice / Clasificate** – protejate conform reglementărilor NATO, EIB sau UE.

Fiecare nivel implică măsuri specifice de stocare, transmitere, criptare și audit.

7. Prevenirea incidentelor cibernetice

CODATA implementează controale tehnice și organizaționale pentru prevenirea incidentelor:

- firewall-uri avansate, IDS/IPS și gateway-uri securizate;
- segmentarea și izolarea traficului de rețea;
- soluții antivirus și antimalware actualizate;
- monitorizarea comportamentului utilizatorilor și a traficului (UEBA/SIEM);

- detectarea și blocarea tentativelor de phishing și ransomware;
- restricționarea accesului la dispozitive externe și aplicații neautorizate.

8. Răspuns la incidente și continuitate

CODATA are un **Plan de Răspuns la Incidente (IRP)** care prevede:

1. **Detecție și alertare automată** în timp real;
2. **Analiză și clasificare a incidentului** (minor, major, critic);
3. **Izolare rapidă a sistemului afectat**;
4. **Restaurare sigură din backup verificat**;
5. **Raportare internă și externă (GDPR, NIS2)** în termen de 72 de ore;
6. **Audit post-incident** pentru prevenirea recurenței.

Echipa de răspuns la incidente (IRT) include experți IT, securitate, juridic și comunicare.

9. Securitatea partenerilor și a lanțului de aprovizionare

Toți furnizorii și subcontractorii CODATA trebuie să respecte:

- clauze contractuale de securitate informatică;
- verificări periodice de conformitate;
- standarde minime de protecție (ISO 27001, NIS2, GDPR). Partenerii care gestionează date sensibile sunt evaluați și monitorizați prin proceduri KYC/KYT (Know Your Partner / Technology).

10. Responsabilități

Responsabilitățile principale sunt:

- **Consiliul de Administrație** – definește politica și aprobă resursele;
- **Chief Information Security Officer (CISO)** – implementează și coordonează măsurile tehnice;
- **Ofițerul de Conformitate (Compliance Officer)** – monitorizează respectarea legislației și contractelor;
- **Departamentul IT** – gestionează infrastructura și aplică măsurile de securitate;
- **Toți angajații** – trebuie să respecte regulile și să raporteze imediat incidentele la **security@codata.ro**

11. Sancțiuni

Încălcarea politicii de securitate informatică poate conduce la:

- suspendarea accesului la sistemele IT;
- sancțiuni disciplinare și financiare;
- răspundere civilă sau penală, în funcție de gravitate. CODATA aplică principiul **„Securitate completă, fără excepții”**.

X. INFORMATION SECURITY AND DIGITAL INFRASTRUCTURE PROTECTION POLICY

1. Purpose

This policy protects CODATA Software Solutions' digital infrastructure, data, and systems against unauthorized access, loss, or compromise. CODATA views cybersecurity as a **strategic priority** and an essential condition for safe, compliant operations.

2. Scope

The policy applies to:

- all IT systems (servers, applications, networks, cloud environments);
- employees, contractors, and partners with system access;
- all national and international projects, including classified or EIB/NATO-funded initiatives.

3. Objectives

CODATA aims to:

1. secure data and digital assets;
2. ensure confidentiality, integrity, and availability (CIA);
3. prevent cyber incidents;
4. respond rapidly to attacks;

5. maintain compliance with legal and contractual obligations.

4. Legal Framework and Standards

This policy complies with:

- **ISO/IEC 27001:2022**;
- **EU Directive 2022/2555 (NIS2)**;
- **EU GDPR (2016/679)**;
- **CIS Controls v8**;
- **NATO STANAG 4774/4778**;
- **National cybersecurity and critical infrastructure laws**.

5. Security Principles

CODATA follows key principles:

1. **Least privilege, maximum control**;
2. **Zero Trust Architecture**;
3. **Network segregation**;
4. **Multi-factor authentication (MFA)**;
5. **End-to-end encryption**;
6. **Continuous monitoring and auditing**;
7. **Patch management**;
8. **Business continuity and disaster recovery plans**.

6. Data Classification

CODATA classifies information as:

1. **Public**
2. **Internal**
3. **Confidential**
4. **Critical / Classified** (NATO, EU, or EIB standards).

Each level has specific handling, storage, and encryption controls.

7. Cyber Incident Prevention

Measures include:

- firewalls, IDS/IPS, and secure gateways;
- segmented network architecture;
- up-to-date antivirus and endpoint protection;
- behavioral monitoring (UEBA/SIEM);
- phishing and ransomware detection;
- restrictions on removable media and unapproved applications.

8. Incident Response and Continuity

CODATA's **Incident Response Plan (IRP)** covers:

1. detection and alerting;
2. incident classification;
3. containment and isolation;
4. restoration from verified backups;
5. reporting within 72 hours (GDPR/NIS2);
6. post-incident review.

The IRT (Incident Response Team) includes IT, Legal, Security, and Communication leads.

9. Partner and Supply Chain Security

All CODATA suppliers must comply with:

- cybersecurity clauses in contracts;
- regular compliance assessments;
- minimum protection standards (ISO 27001, NIS2, GDPR).

Partners handling sensitive data are vetted under **KYC/KYT** procedures.

10. Responsibilities

- **Board of Directors:** defines strategy and approves resources;
- **CISO:** implements and manages technical controls;
- **Compliance Officer:** monitors legal and contractual obligations;
- **IT Department:** enforces technical safeguards;
- **All Employees:** must adhere to rules and report incidents to **security@codata.ro**

11. Sanctions

Policy violations may lead to:

- access suspension;
- disciplinary and financial sanctions;
- civil or criminal liability.

CODATA enforces the principle **"Complete Security – No Exceptions."**

XI. POLITICA PRIVIND INTEGRITATEA PARTENERILOR ȘI DUE DILIGENCE (KYC / KYB / KYT)

1. Scopul politicii

Scopul acestei politici este de a asigura că toți partenerii, clienții, furnizorii și subcontractorii CODATA Software Solutions respectă standarde ridicate de etică, legalitate și integritate. CODATA aplică proceduri stricte de **due diligence** pentru a preveni colaborarea cu entități implicate în activități ilegale, corupție, fraudă, spălare de bani, conflicte de interese sau încălcări ale sancțiunilor internaționale.

2. Domeniul de aplicare

Politica se aplică:

- tuturor entităților juridice și persoanelor fizice cu care CODATA colaborează;
- tuturor etapelor de contractare, achiziție, subantrepriză sau parteneriat strategic;
- tuturor tranzacțiilor financiare și tehnice din cadrul proiectelor CODATA;
- filialelor și companiilor asociate CODATA, atât în România, cât și la nivel internațional.

3. Principii generale

Evaluarea partenerilor se bazează pe următoarele principii:

1. **Integritate și transparență totală** – colaborăm doar cu entități care demonstrează comportament etic și legal.

2. **Diligență rezonabilă (Due Diligence)** – verificăm identitatea, reputația și conformitatea fiecărui partener.
3. **Evaluare proporțională cu riscul** – intensitatea verificării se stabilește în funcție de profilul de risc (scăzut, mediu, ridicat).
4. **Documentare completă** – toate verificările sunt înregistrate, arhivate și disponibile pentru audit.
5. **Monitorizare continuă** – partenerii sunt reevaluati periodic, mai ales în proiecte strategice.

4. Etapele procesului KYC / KYB / KYT

CODATA implementează un proces standardizat în trei etape:

a) KYC – Know Your Customer

- verificarea identității partenerului și a reprezentanților legali;
- analiza datelor din registre comerciale, baze publice și surse oficiale (ONRC, VIES, UE, ONU, OFAC);
- confirmarea existenței juridice, a adresei și a obiectului de activitate;
- verificarea integrității persoanelor-cheie și a istoricului de conformitate.

b) KYB – Know Your Business

- evaluarea structurii acționariatului și identificarea **beneficiarilor reali (UBO)**;
- analiza riscului de corupție, spălare de bani sau sancțiuni economice;
- verificarea certificărilor, autorizațiilor și reputației în piață;
- analiza relațiilor anterioare cu CODATA sau alți parteneri publici.

c) KYT – Know Your Transaction

- analiza scopului și legalității tranzacțiilor financiare;
- verificarea proveniență fondurilor;
- monitorizarea transferurilor internaționale, în special către jurisdicții cu risc ridicat;
- aplicarea controalelor suplimentare pentru plăți suspecte sau neobișnuite.

5. Evaluarea riscurilor partenerilor

Fiecare partener este încadrat într-un nivel de risc:

- **Risc scăzut:** entități europene, reglementate, cu istoric pozitiv și parteneriate repetate.
- **Risc mediu:** parteneri noi, fără istoric în piață sau din domenii sensibile (IT, AI, finanțe).
- **Risc ridicat:** entități din țări non-UE, paradisuri fiscale, sau implicate anterior în investigații juridice.

Pentru partenerii cu risc ridicat, colaborarea necesită aprobarea expresă a Directorului General și a Ofițerului de Conformitate.

6. Surse de verificare și instrumente utilizate

CODATA utilizează:

- baze de date oficiale (ONRC, EU Sanctions List, OFAC, Interpol, Transparency International);
- platforme KYC/KYB specializate;
- verificări interne reputaționale;
- audituri de teren sau evaluări directe pentru contracte strategice.

Toate datele sunt colectate și procesate în conformitate cu **GDPR** și legislația privind protecția datelor.

7. Relațiile cu partenerii și transparența contractuală

CODATA cere tuturor partenerilor:

- semnarea unui **Angajament de integritate și conformitate**;
- respectarea **Codului de Conduită CODATA**;
- declararea eventualelor conflicte de interese;
- colaborare totală în cadrul oricărei investigații de conformitate;
- notificarea imediată în cazul unor modificări de structură, proprietate sau sancțiuni.

8. Monitorizare și reevaluare continuă

Partenerii sunt monitorizați periodic prin:

- analize automate ale bazelor de date de sancțiuni;
- audituri tematice;
- actualizarea documentației la fiecare 12 luni;
- reevaluare completă în caz de modificare majoră (proprietar, sediu, jurisdicție, incident juridic).

9. Sancțiuni și încetarea colaborării

CODATA își rezervă dreptul de a suspenda sau înceta imediat colaborarea cu orice partener care:

- furnizează informații false sau incomplete;
- refuză cooperarea în procesul de due diligence;
- este implicat în activități ilegale sau neetice;
- încalcă legislația privind sancțiunile internaționale.

Decizia de încetare este documentată și comunicată oficial partenerului.

XI. PARTNER INTEGRITY AND DUE DILIGENCE POLICY (KYC / KYB / KYT)

1. Purpose

This policy ensures that all CODATA Software Solutions partners, clients, suppliers, and subcontractors meet the highest ethical and legal standards. CODATA applies rigorous **due diligence procedures** to prevent collaboration with entities involved in illegal, corrupt, or unethical activities.

2. Scope

Applies to:

- all entities and individuals collaborating with CODATA;
- all procurement, subcontracting, or partnership activities;
- all financial and technical transactions;
- all CODATA subsidiaries and affiliates, domestic and international.

3. Core Principles

CODATA's partner evaluation is guided by:

1. **Integrity and transparency**;
2. **Reasonable diligence (Due Diligence)**;
3. **Risk-based assessment**;
4. **Complete documentation**;
5. **Ongoing monitoring**.

4. KYC / KYB / KYT Process

KYC – Know Your Customer

- verify partner identity and legal representatives;
- check official registries and sanction databases (EU, UN, OFAC);
- confirm legal existence and activity scope;
- assess integrity and compliance history.

KYB – Know Your Business

- identify ultimate beneficial owners (UBOs);
- assess corruption, AML, and sanction risks;
- verify licenses, certifications, and reputation;
- review previous relationships with CODATA.

KYT – Know Your Transaction

- analyze purpose and legality of financial operations;
- verify fund origin;
- monitor cross-border transactions;
- apply enhanced controls to suspicious or high-value transfers.

5. Risk Levels

Each partner is classified as:

- **Low risk:** established EU entities with strong compliance history.
- **Medium risk:** new or untested partners in sensitive industries.
- **High risk:** entities from non-EU or sanctioned jurisdictions.

High-risk engagements require formal approval from CODATA's Compliance and Executive teams.

6. Verification Sources

CODATA uses:

- official databases (EU, OFAC, Interpol, Transparency International);
- specialized KYC/KYB tools;
- internal reputation analysis;
- on-site audits for strategic contracts.

All data is handled in compliance with **GDPR** and data protection laws.

7. Partner Relations and Transparency

All partners must:

- sign a **Compliance and Integrity Agreement**;
- comply with the **CODATA Code of Conduct**;
- declare conflicts of interest;
- fully cooperate with compliance investigations;
- promptly notify any changes in ownership or legal status.

8. Monitoring and Review

Partners are reviewed periodically through:

- automated sanctions screening;
- targeted audits;
- yearly documentation updates;
- re-evaluation after structural or legal changes.

9. Sanctions

CODATA may suspend or terminate collaboration with any partner that:

- provides false or incomplete information;
- refuses to cooperate in due diligence;
- engages in illegal or unethical behavior;
- violates international sanctions.

Decisions are documented and communicated formally.

XII. POLITICA PRIVIND COMUNICAREA PUBLICĂ ȘI RELAȚIILE MEDIA

1. Scopul politicii

Scopul acestei politici este de a stabili reguli clare privind comunicarea publică și relațiile media, pentru a asigura un mesaj unitar, profesionist și conform valorilor CODATA Software Solutions. Comunicarea externă reprezintă o componentă strategică a reputației și trebuie gestionată cu atenție, transparență și responsabilitate.

2. Domeniul de aplicare

Politica se aplică tuturor:

- angajaților, colaboratorilor și reprezentanților CODATA;
- partenerilor implicați în proiecte care comunică în numele companiei;
- canalelor oficiale (website, LinkedIn, social media, conferințe, presă, evenimente);
- comunicărilor scrise, orale sau digitale privind activitățile CODATA.

3. Principii generale de comunicare

CODATA își bazează comunicarea pe următoarele principii:

1. **Acuratețe** – informațiile comunicate trebuie să fie corecte și verificabile.
2. **Coerență** – toate mesajele publice trebuie să reflecte identitatea și valorile companiei.
3. **Transparență** – comunicarea trebuie să fie clară și onestă, fără ambiguități.
4. **Responsabilitate** – declarațiile externe trebuie făcute doar de persoane autorizate.
5. **Confidențialitate** – informațiile interne sau contractuale nu se divulgă fără aprobare.

4. Comunicarea oficială

Doar persoanele desemnate de conducere pot face declarații oficiale în numele CODATA:

- Fondatorul și Directorul General;
- Directorul de Comunicare;
- Managerii de proiect autorizați pentru declarații tehnice.

Orice comunicare externă trebuie aprobată în prealabil de **Departamentul de Comunicare** sau **Ofițerul de Conformitate**, pentru a evita interpretările greșite sau divulgarea de informații sensibile.

5. Relația cu mass-media

În relația cu presa:

- toate solicitările media trebuie direcționate către **media@codata.ro**;
- declarațiile oficiale se oferă doar în scris sau în cadrul interviurilor aprobate;
- materialele de presă trebuie să fie exacte, clare și lipsite de opinii personale;
- comentariile publice despre parteneri, clienți sau instituții publice sunt interzise fără mandatul conducerii;
- participarea la emisiuni, evenimente sau conferințe se face doar cu aprobare prealabilă.

6. Rețele sociale și comunicare digitală

CODATA recunoaște importanța rețelelor sociale (LinkedIn, X, Facebook, YouTube etc.) ca instrumente de promovare și comunicare. Reguli:

1. Angajații pot promova activitățile companiei doar folosind informații publice.
2. Este interzisă publicarea de date confidențiale, imagini din proiecte, contracte sau corespondență internă.
3. Opiniile personale trebuie clar diferențiate de cele ale companiei.
4. Comentariile despre instituții publice, parteneri sau competitori sunt interzise.
5. Postările oficiale trebuie aprobate de Departamentul de Comunicare.
6. Toate conturile corporative sunt administrate centralizat, cu acces controlat.

7. Comunicarea în situații de criză

În cazul unui incident de securitate, litigiu sau criză reputațională:

- doar echipa desemnată de criză (PR, juridic, conformitate) poate comunica public;
- toate mesajele trebuie coordonate și aprobate în prealabil;
- se evită reacțiile spontane, interpretările și comentariile neoficiale;
- se asigură coerența între comunicarea internă și cea externă.

Scopul este gestionarea controlată a informațiilor și protejarea reputației companiei.

8. Protejarea imaginii CODATA

Fiecare angajat este un ambasador al brandului. Comportamentul, limbajul și atitudinea în mediul public trebuie să reflecte profesionalismul și valorile companiei. Este interzisă:

- folosirea logo-ului, denumirii sau identității vizuale în scopuri personale;
- participarea la dezbateri publice în numele companiei fără autorizare;
- publicarea de materiale ce pot afecta imaginea CODATA sau a partenerilor săi.

9. Sancțiuni

Încălcarea politicii de comunicare poate atrage:

- retragerea dreptului de a comunica în numele companiei;
- sancțiuni disciplinare;
- răspundere juridică în caz de prejudiciu.

CODATA promovează o cultură a **comunicării profesionale, controlate și transparente**, care consolidează încrederea publică.

XII. PUBLIC COMMUNICATION AND MEDIA RELATIONS POLICY

1. Purpose

This policy establishes clear rules for public communication and media relations to ensure consistent, professional, and responsible representation of CODATA Software Solutions. External communication directly influences CODATA's reputation and must be handled with accuracy and integrity.

2. Scope

Applies to:

- all employees, collaborators, and representatives;
- all communication channels (website, LinkedIn, media, events);
- all written, oral, and digital communications regarding CODATA activities.

3. Core Principles

CODATA's communication is guided by:

1. **Accuracy** – share only verified, factual information.
2. **Consistency** – ensure unified corporate messaging.
3. **Transparency** – communicate openly and clearly.
4. **Responsibility** – only authorized representatives may speak on behalf of CODATA.
5. **Confidentiality** – internal and client data must not be disclosed.

4. Official Communication

Only authorized personnel may issue public statements:

- Founder & CEO;
- Communication Director;
- Project Managers with written authorization.

All external communications must be pre-approved by the **Communication Department** or **Compliance Officer**.

5. Media Relations

In dealing with the media:

- all requests must be directed to **media@codata.ro**;
- official statements are written or approved interviews only;
- materials must be factual and neutral;
- public commentary about partners or institutions is prohibited;
- participation in public events requires prior authorization.

6. Social Media and Digital Communication

CODATA encourages responsible social media engagement:

1. Share only public and verified information.
2. Do not post internal data, images, or project details.
3. Personal opinions must not be presented as company views.
4. Avoid public discussions about clients or competitors.
5. Official posts require Communication Department approval.
6. Corporate accounts are centrally managed and monitored.

7. Crisis Communication

During security incidents or reputational crises:

- only the designated crisis team may issue statements;
- all messages must be approved in advance;
- spontaneous or unofficial comments are forbidden;
- internal and external communication must be aligned.

Objective: protect the company's reputation and ensure factual accuracy.

8. Corporate Image Protection

Every employee represents CODATA. Public conduct must reflect professionalism and respect for company values. It is forbidden to:

- use the logo or brand identity for personal purposes;
- speak publicly on behalf of CODATA without authorization;

- post content that damages the company's or partners' image.

9. Sanctions

Breaches of this policy may result in:

- withdrawal of communication privileges;
- disciplinary action;
- legal liability for reputational damage.

CODATA promotes a culture of **professional, accurate, and transparent communication** that strengthens public trust.

XIII. POLITICA PRIVIND SĂNĂTATEA, SIGURANȚA ȘI BUNĂSTAREA LA LOCUL DE MUNCĂ

1. Scopul politicii

Scopul acestei politici este de a proteja sănătatea, siguranța și bunăstarea tuturor angajaților CODATA Software Solutions, precum și a colaboratorilor și vizitatorilor care interacționează cu mediul nostru de lucru.
CODATA consideră siguranța angajaților o prioritate absolută și promovează o cultură organizațională bazată pe prevenție, responsabilitate și respect pentru oameni.

2. Domeniul de aplicare

Politica se aplică:

- tuturor angajaților CODATA, indiferent de poziție sau departament;
- colaboratorilor externi, partenerilor și vizitatorilor care lucrează în sediile CODATA;
- tuturor locațiilor, birourilor și spațiilor tehnice operate de companie;
- proiectelor desfășurate pe teren sau la sediul clienților.

3. Obiective

CODATA urmărește:

1. menținerea unui mediu de lucru sigur și sănătos;
2. prevenirea accidentelor, bolilor profesionale și stresului ocupațional;
3. promovarea bunăstării mentale și fizice a angajaților;
4. instruirea continuă în domeniul securității și sănătății;
5. asigurarea conformității cu legislația națională și internațională.

4. Principii fundamentale

1. **Prevenția înainte de reacție** – identificarea și eliminarea riscurilor înainte de apariția incidentelor.
2. **Responsabilitate comună** – siguranța este o obligație partajată între angajați și conducere.
3. **Comunicare deschisă** – orice risc sau incident trebuie raportat imediat.
4. **Respect și demnitate** – mediul de lucru trebuie să fie lipsit de hărțuire, discriminare sau stres inutil.
5. **Echilibru profesional-personal** – promovarea unui ritm de lucru sustenabil, cu respectarea timpului liber.

5. Măsuri de securitate la locul de muncă

CODATA implementează măsuri concrete pentru siguranța fizică și digitală a angajaților:

- verificarea periodică a echipamentelor electrice și IT;
- semnalizarea clară a căilor de evacuare și a punctelor de prim ajutor;
- respectarea normelor privind incendii, cutremure și evacuare de urgență;
- controale medicale periodice;
- echipamente ergonomice pentru lucrul la birou (scaune reglabile, monitoare, iluminare corectă);
- politici de lucru hibrid și telemuncă, cu reguli clare de securitate și sănătate.

6. Sănătate mentală și stres digital

CODATA recunoaște impactul stresului digital asupra performanței și sănătății angajaților. Compania:

- promovează pauzele regulate și limitele rezonabile de timp petrecut în fața ecranelor;
- oferă sprijin psihologic și consiliere pentru angajați, la cerere;
- evită suprasolicitarea prin planificare realistă a proiectelor;
- încurajează echilibrul între viața profesională și cea personală.

7. Raportarea incidentelor

Orice accident, incident de securitate sau condiție periculoasă trebuie raportată imediat la:

- **hr@codata.ro**
- **safety@codata.ro**
- superiorul direct sau Ofițerul de Conformitate.

Toate raportările sunt investigate prompt și tratate cu confidențialitate, fără consecințe negative pentru persoana care a semnalat.

8. Formare și instruire

CODATA organizează sesiuni periodice de instruire privind:

- sănătatea și securitatea în muncă;
- acordarea primului ajutor;
- gestionarea stresului și ergonomia digitală;

- reacția în situații de urgență.

Participarea la aceste programe este obligatorie pentru toți angajații.

9. Monitorizare și îmbunătățire continuă

CODATA evaluează anual performanța în domeniul sănătății și securității prin:

- audituri interne și externe;
- chestionare de satisfacție și feedback anonim;
- analiza incidentelor și implementarea măsurilor preventive.

Rezultatele sunt utilizate pentru îmbunătățirea continuă a condițiilor de muncă.

10. Angajamentul conducerii

Conducerea CODATA își asumă personal responsabilitatea de a oferi resursele, echipamentele și sprijinul necesar pentru menținerea unui mediu sigur și sănătos. Siguranța și bunăstarea angajaților sunt valori fundamentale, nu doar obligații legale.

XIII. HEALTH, SAFETY, AND WELL-BEING POLICY

1. Purpose

This policy protects the health, safety, and well-being of all CODATA Software Solutions employees, contractors, and visitors. CODATA views safety as a **core organizational value** and promotes a proactive culture of prevention and respect.

2. Scope

Applies to:

- all CODATA employees and contractors;
- all office and technical locations;
- client-site activities and hybrid work setups.

3. Objectives

CODATA aims to:

1. maintain a safe and healthy workplace;
2. prevent accidents and occupational illnesses;
3. promote mental and physical well-being;
4. provide continuous safety training;
5. ensure legal and regulatory compliance.

4. Core Principles

1. **Prevention first** – identify and mitigate risks proactively.
2. **Shared responsibility** – safety is everyone's duty.
3. **Open communication** – report risks immediately.

4. **Respect and dignity** – a harassment-free, healthy environment.
5. **Work-life balance** – sustainable productivity and rest.

5. Workplace Safety Measures

CODATA implements:

- regular inspection of electrical and IT equipment;
- visible emergency exits and first aid stations;
- compliance with fire and earthquake safety norms;
- regular medical check-ups;
- ergonomic furniture and lighting;
- hybrid work guidelines with secure remote environments.

6. Mental Health and Digital Stress

CODATA acknowledges digital overload risks and:

- encourages regular breaks and healthy screen time limits;
- provides access to counseling support;
- plans projects realistically to prevent burnout;
- promotes work-life balance across teams.

7. Incident Reporting

Any workplace accident or hazard must be reported immediately to:

- **hr@codata.ro**
- **safety@codata.ro**
- the direct supervisor or Compliance Officer.

Reports are handled confidentially, without retaliation.

8. Training and Awareness

CODATA provides ongoing training in:

- workplace safety;
- first aid and emergency response;
- stress management and ergonomics.

Participation is mandatory for all staff.

9. Monitoring and Continuous Improvement

Annual evaluations include:

- internal and external audits;

- anonymous employee surveys;
- corrective and preventive action reviews.

Findings are used to enhance the safety management system.

10. Management Commitment

The Board of Directors ensures that all necessary resources, equipment, and support are available to maintain a safe, healthy, and sustainable work environment. **People come first. Safety is non-negotiable.**

XIV. POLITICA PRIVIND DIVERSITATEA, INCLUZIUNEA ȘI EGALITATEA DE ȘANSE

1. Scopul politicii

Scopul acestei politici este de a promova un mediu de lucru divers, incluziv și echitabil în cadrul CODATA Software Solutions, în care fiecare persoană este tratată cu respect și are șanse egale de dezvoltare profesională.
CODATA consideră diversitatea o sursă de inovație, iar incluziunea – o condiție pentru performanță și sustenabilitate.

2. Domeniul de aplicare

Politica se aplică:

- tuturor angajaților, candidaților și colaboratorilor CODATA;
- tuturor proceselor de recrutare, promovare, formare și recompensare;
- relațiilor interne și externe ale companiei;
- tuturor filialelor și proiectelor CODATA, indiferent de locație.

3. Principii fundamentale

1. **Egalitate de șanse** – toți angajații beneficiază de tratament echitabil, fără discriminare.
2. **Respect reciproc** – fiecare persoană este valorizată pentru contribuția și identitatea sa.
3. **Diversitate culturală** – CODATA promovează echipe mixte, multidisciplinare și interculturale.
4. **Incluziune activă** – compania încurajează participarea tuturor, indiferent de origini sau convingeri.
5. **Toleranță zero** – nu se acceptă niciun comportament discriminatoriu, ofensator sau excludent.

4. Domenii de aplicare practică

CODATA aplică principiile diversității în toate etapele vieții profesionale:

a) Recrutare și selecție

- procesele de recrutare se bazează exclusiv pe competențe și merit;
- anunțurile de angajare folosesc un limbaj neutru și incluziv;
- comisiile de recrutare sunt instruite pentru a evita prejudecățile inconștiente.

b) Dezvoltare și promovare

- acces egal la programe de training, mentorat și certificare;
- evaluarea performanței se face obiectiv, pe baza rezultatelor;
- oportunitățile de promovare sunt deschise tuturor, fără favoritisme.

c) Mediu de lucru

- respect reciproc în toate interacțiunile;
- interzicerea oricărei forme de hărțuire, discriminare sau abuz;
- adaptarea condițiilor de muncă pentru persoane cu dizabilități sau nevoi speciale;
- susținerea echilibrului între viața profesională și cea personală.

5. Angajamentul conducerii

Conducerea CODATA:

- asigură aplicarea efectivă a politicii de diversitate și incluziune;
- oferă resurse pentru programe interne de formare și conștientizare;
- evaluează anual indicatorii de diversitate și satisfacție;
- promovează femeile și tinerii în roluri de leadership și inovare;
- susține inițiativele care combat discriminarea în mediul tehnologic și public.

6. Mecanisme de raportare

Orice formă de discriminare, excludere sau comportament ofensator poate fi raportată confidențial prin:

- **email:** hr@codata.ro
- **platforma Speak-Up** – anonimă, securizată și monitorizată de Ofițerul de Conformitate.

CODATA garantează protecția completă a persoanelor care raportează de bună credință.

7. Monitorizare și îmbunătățire continuă

Politica este revizuită anual, pe baza:

- feedbackului angajaților;
- evoluției cadrului legal;
- obiectivelor ESG asumate de companie.

CODATA publică periodic indicatori de echitate și diversitate în raportul său de guvernanță corporativă.

XIV. DIVERSITY, INCLUSION, AND EQUAL OPPORTUNITY POLICY

1. Purpose

This policy promotes a diverse, inclusive, and equitable work environment at CODATA Software Solutions, ensuring equal treatment and growth opportunities for all. CODATA believes diversity drives innovation, while inclusion ensures sustainable performance.

2. Scope

Applies to:

- all employees, candidates, and contractors;
- all recruitment, training, evaluation, and promotion processes;
- internal and external relations;
- all subsidiaries and international projects.

3. Core Principles

1. **Equal opportunity** – decisions based solely on merit and competence.
2. **Mutual respect** – value every person's identity and contribution.
3. **Cultural diversity** – promote mixed, multidisciplinary, international teams.
4. **Active inclusion** – ensure participation and voice for all employees.
5. **Zero tolerance** – prohibit discrimination, harassment, or exclusion.

4. Application Areas

a) Recruitment and Selection

- merit-based hiring using inclusive language;
- unbiased evaluation by trained panels;
- open and transparent recruitment procedures.

b) Development and Promotion

- equal access to learning, mentoring, and certification;
- objective performance evaluations;
- fair promotion opportunities across all teams.

c) Work Environment

- respect in all interactions;
- protection against harassment or discrimination;
- workplace adaptation for employees with disabilities;
- support for work-life balance.

5. Management Commitment

CODATA's leadership:

- ensures implementation and enforcement of this policy;
- allocates resources for diversity training and awareness;
- evaluates diversity and inclusion indicators annually;
- promotes gender balance and youth leadership;
- supports initiatives combating discrimination in tech and public institutions.

6. Reporting Mechanisms

Discrimination or exclusion can be reported confidentially via:

- **Email:** hr@codata.ro
- **Speak-Up Platform** – anonymous and monitored by the Compliance Officer.

Whistleblowers acting in good faith are fully protected.

7. Monitoring and Continuous Improvement

The policy is reviewed annually based on:

- employee feedback;
- legal developments;
- ESG governance objectives.

CODATA regularly publishes diversity indicators in its corporate sustainability report.

XV. POLITICA PRIVIND GUVERNANȚA CORPORATIVĂ ȘI RESPONSABILITATEA SOCIALĂ (ESG)

1. Scopul politicii

Această politică stabilește principiile și angajamentele CODATA Software Solutions privind **guvernanța corporativă, responsabilitatea socială și sustenabilitatea**. Scopul este asigurarea unei conduceri responsabile, transparente și etice, care contribuie la dezvoltarea durabilă și la creșterea încrederii partenerilor, clienților și comunității.

2. Domeniul de aplicare

Politica se aplică:

- tuturor entităților juridice din cadrul grupului CODATA;
- tuturor angajaților, partenerilor și colaboratorilor;
- tuturor proiectelor publice și private în care CODATA este implicată;
- proceselor interne de management, achiziție, conformitate și raportare.

3. Principiile fundamentale de guvernanță

CODATA adoptă următoarele principii, în conformitate cu **ISO 37000:2021 – Governance of Organizations**:

1. **Transparență** – comunicarea clară și completă a deciziilor, riscurilor și rezultatelor.
2. **Responsabilitate** – asumarea consecințelor acțiunilor și deciziilor la toate nivelurile.
3. **Integritate** – aplicarea principiilor etice în toate activitățile și deciziile companiei.
4. **Eficiență** – utilizarea responsabilă a resurselor pentru rezultate sustenabile.
5. **Echitate** – tratament corect și respectuos pentru toți stakeholderii.
6. **Sustenabilitate** – integrarea obiectivelor economice, sociale și de mediu într-o strategie unitară.

4. Structura de guvernanță

CODATA este organizată conform unui model de guvernanță corporativă modern, cu roluri și responsabilități clar definite:

- **Consiliul de Administrație (Board of Directors)** – stabilește direcția strategică și supraveghează implementarea politicilor ESG;

- **Directorul General (CEO)** – asigură execuția strategiei și coordonarea operațională;
- **Ofițerul de Conformitate (Compliance Officer)** – monitorizează respectarea legislației și codului de etică;
- **Responsabilul ESG** – colectează, analizează și raportează indicatorii de mediu, sociali și guvernanță;
- **Comitetul de Etică și Sustenabilitate** – analizează sesizările interne, propune acțiuni corective și raportează direct Consiliului.

5. Dimensiunea „E" – Mediu (Environment)

CODATA își asumă angajamente concrete privind protecția mediului:

- reducerea amprentei de carbon și a consumului de energie;
- utilizarea tehnologiilor verzi, a echipamentelor eficiente și a infrastructurilor cloud sustenabile;
- eliminarea hârtiei prin digitalizare completă;
- reciclarea echipamentelor IT și colectarea selectivă a deșeurilor;
- raportarea anuală a indicatorilor de mediu și sustenabilitate conform **EU CSRD** (Corporate Sustainability Reporting Directive).

6. Dimensiunea „S" – Social (Responsabilitate socială)

CODATA contribuie activ la dezvoltarea comunității și la bunăstarea socială prin:

- respectarea drepturilor fundamentale ale omului;
- crearea de locuri de muncă sigure și echitabile;
- sprijinirea educației digitale și formării profesionale;
- parteneriate cu universități, ONG-uri și instituții publice pentru proiecte educaționale;
- campanii de sprijin pentru grupurile vulnerabile și promovarea incluziunii sociale.

7. Dimensiunea „G" – Governance (Guvernanță etică)

CODATA se angajează să mențină standarde înalte de etică și conformitate:

- aplicarea principiilor anti-corupție și anti-fraudă (ISO 37001);
- control intern riguros asupra deciziilor financiare și operaționale;
- audituri periodice independente;
- respectarea legislației privind protecția datelor, achizițiile publice și concurența;
- protejarea avertizorilor de integritate (whistleblowers).

8. Obiective ESG măsurabile

CODATA stabilește anual indicatori de performanță ESG, care sunt integrați în planurile de management:

- **E:** reducerea cu 10% a consumului energetic anual per angajat;
- **S:** creșterea procentului de femei în poziții de conducere la minimum 40%;
- **G:** zero incidente de neconformitate majoră și audit ESG pozitiv anual.

9. Raportare și transparență

CODATA publică anual **Raportul ESG și de guvernanță corporativă**, care include:

- performanța în domeniul mediu, social și etic;
- obiectivele și acțiunile implementate;
- indicatorii cheie și progresele măsurabile;
- rezultatele auditului de sustenabilitate.

Raportul este disponibil pe site-ul companiei și transmis partenerilor instituționali.

10. Angajamentul conducerii

Conducerea CODATA se angajează să:

- asigure resursele și suportul pentru implementarea politicii ESG;
- promoveze responsabilitatea socială și inovația etică;
- integreze principiile ESG în toate deciziile strategice;
- contribuie la crearea unei economii digitale sustenabile și echitabile.

CODATA crede într-un model de business unde **etica, performanța și sustenabilitatea merg împreună**.

XV. CORPORATE GOVERNANCE AND SOCIAL RESPONSIBILITY (ESG) POLICY

1. Purpose

This policy defines CODATA Software Solutions' commitment to **corporate governance, social responsibility and sustainability**. Its purpose is to ensure ethical, transparent, and responsible leadership aligned with long-term value creation.

2. Scope

Applies to:

- all CODATA entities and subsidiaries;
- employees, partners, and contractors;
- all public and private projects;
- all management, compliance, and reporting processes.

3. Governance Principles

According to **ISO 37000**, CODATA adheres to:

1. **Transparency** – clear and open decision-making;
2. **Accountability** – responsibility for all outcomes;
3. **Integrity** – ethical conduct in every activity;
4. **Efficiency** – responsible use of resources;
5. **Fairness** – equitable treatment of stakeholders;
6. **Sustainability** – balance between profit, people, and planet.

4. Governance Structure

- **Board of Directors** – defines strategy and oversees ESG implementation;
- **CEO** – ensures operational execution;
- **Compliance Officer** – monitors ethics and regulations;
- **ESG Manager** – collects and reports ESG data;
- **Ethics and Sustainability Committee** – evaluates compliance and proposes improvements.

5. Environmental (E)

CODATA commits to:

- lowering its carbon footprint and energy consumption;
- using green, cloud-based, and efficient technologies;
- achieving full paperless operations;
- recycling and waste reduction;
- reporting under the **EU CSRD framework**.

6. Social (S)

CODATA contributes to society by:

- respecting human rights;
- creating fair and safe workplaces;
- supporting digital education and training;
- collaborating with universities and NGOs;
- running inclusion and community impact programs.

7. Governance (G)

CODATA ensures:

- anti-corruption compliance (ISO 37001);
- strong internal financial and operational controls;
- independent audits;
- GDPR, public procurement, and competition compliance;
- whistleblower protection.

8. ESG Performance Indicators

Annual measurable goals:

- **E:** -10% energy use per employee;
- **S:** ≥40% women in leadership roles;
- **G:** 100% compliance and positive ESG audit.

9. Reporting and Transparency

CODATA issues an annual **ESG & Governance Report**, including:

- environmental and social performance;
- measurable targets and actions;
- audit results and sustainability metrics.

It is publicly available and shared with institutional partners.

10. Management Commitment

Leadership ensures:

- adequate resources and oversight for ESG initiatives;
- integration of ethics and sustainability in all decisions;
- continuous alignment with EU and international ESG standards.

CODATA stands for a model of **ethical innovation and sustainable digital transformation**.

XVI. DISPOZIȚII FINALE

1. Aplicabilitate

Prezentul **Cod de Conduită și Etică în Afaceri** se aplică tuturor angajaților, colaboratorilor, partenerilor contractuali, consultanților și reprezentanților CODATA Software Solutions, indiferent de poziție, durată a colaborării sau locație. Respectarea Codului este **obligatorie** și reprezintă o condiție de apartenență la organizație.

2. Responsabilitate și implementare

Responsabilitatea pentru aplicarea și respectarea acestui Cod revine:

- **Consiliului de Administrație**, care aprobă și monitorizează implementarea sa;
- **Directorului General**, care asigură integrarea principiilor etice în toate procesele operaționale;
- **Ofițerului de Conformitate**, care coordonează instruirea, raportarea și monitorizarea incidentelor;
- **Tuturor angajaților CODATA**, care au obligația de a acționa în conformitate cu principiile acestui document.

Fiecare angajat semnează o **declarație de luare la cunoștință** la momentul angajării sau al actualizării Codului.

3. Revizuirea periodică

Codul este revizuit **anual** sau ori de câte ori apar modificări legislative, standarde noi sau evenimente semnificative care impun adaptarea sa. Propunerile de modificare sunt analizate de **Comitetul de Etică și Sustenabilitate**, apoi aprobate de **Consiliul de Administrație**.

4. Mecanisme de raportare

Orice încălcare, suspiciune sau nerespectare a prevederilor Codului poate fi raportată confidențial prin:

- **Email:** compliance@codata.ro
- **Platforma Speak-Up (anonimă și securizată)**
- **Contact direct cu Ofițerul de Conformitate**.

CODATA garantează protecția totală a persoanelor care raportează de bună credință.

5. Confidențialitate și protecția avertizorilor

Toate raportările sunt tratate cu **discreție absolută**. Este strict interzisă orice formă de represalii împotriva angajaților care semnalează nereguli. CODATA aplică integral prevederile **Legii nr. 361/2022 privind protecția avertizorilor în interes public** și ale Directivei (UE) 2019/1937.

6. Intrarea în vigoare

Acest Cod intră în vigoare la data **1 septembrie 2025**, în urma aprobării de către managementul CODATA Software Solutions. Toate versiunile anterioare sunt considerate abrogate de la aceeași dată.

7. Aprobarea oficială

Codul de Conduită și Etică în Afaceri – versiunea 2025 a fost adoptat în ședința Consiliului de Administrație din data de **1 septembrie 2025**, semnat de:

Horia SABO
Director General
CODATA Software Solutions
București, România

XVI. FINAL PROVISIONS

1. Applicability

This **Code of Conduct and Business Ethics** applies to all employees, contractors, partners, consultants, and representatives of CODATA Software Solutions, regardless of role or contract type. Compliance is **mandatory** and a condition of employment or collaboration.

2. Responsibility and Implementation

Responsibility for enforcement lies with:

- **Board of Directors** – approves and oversees implementation;
- **CEO** – integrates ethical principles into operations;
- **Compliance Officer** – manages training, reporting, and monitoring;
- **All Employees** – act in full accordance with this Code.

Each employee signs an **acknowledgment statement** upon hiring or when the Code is updated.

3. Periodic Review

The Code is reviewed **annually** or whenever required by legal or organizational changes. Proposed revisions are evaluated by the **Ethics and Sustainability Committee** and approved by the **Board of Directors**.

4. Reporting Mechanisms

Any suspected or confirmed violation can be reported confidentially via:

- **Email:** compliance@codata.ro
- **Speak-Up Platform (anonymous and secure)**
- **Direct contact with the Compliance Officer**.

CODATA guarantees full protection for good-faith whistleblowers.

5. Confidentiality and Whistleblower Protection

All reports are handled **strictly confidentially**. Retaliation against whistleblowers is strictly prohibited. CODATA fully complies with **Romanian Law 361/2022** and **EU Directive 2019/1937** on whistleblower protection.

6. Entry into Force

This Code enters into force on **September 1st, 2025**, following approval by the **CODATA Board of Management**.
All previous versions are hereby repealed.

7. Official Approval

Adopted by the Board of Management on **September 1st, 2025** and signed by:

Horia SABO
General Manager
CODATA Software Solutions
Bucharest, Romania