Un deceniu de transformare în domeniul protecției datelor: cum a evoluat practica de la conformarea la cerințele GDPR la construirea unor mecanisme sofisticate de guvernanța a informațiilor | De vorba cu Alexandra Nania, Managing Associate ZRVP, despre maturizarea pieței, noile exigențe ale companiilor și temele care ar putea defini urmatorii zece ani

La zece ani de la intrarea în vigoare a GDPR, protecția datelor a încetat sa mai fie o simpla chestiune de conformare. Pentru companiile din România, datele au devenit un element central al guvernanței organizaționale, al managementului riscurilor și al transformarii digitale, odata cu rolul tot mai important pe care îl joaca în fundamentarea deciziilor de business. Pe acest fond, presiunea de reglementare s-a intensificat: AI Act a intrat în vigoare în 2024, NIS2 a adus obligații noi de securitate cibernetica, iar autoritatea româna de supraveghere a aplicat peste 80 de sancțiuni numai în 2024.În acest peisaj, rolul avocatului specializat în protecția datelor s-a schimbat profund, de la interpret al normelor la partener în deciziile strategice ale clienților.

Despre felul în care arata astazi practica de protecția datelor și încotro se îndreapta, *Biz*Lawyer a discutat cu **Alexandra Nania**, *Managing Associate ZRVP*. Discuția a acoperit maturizarea pieței, intersecția dintre GDPR și AI Act, riscurile concrete ale proiectelor de inteligența artificiala, felul în care autoritațile verifica astazi companiile și temele care vor defini urmatorul deceniu al protecției datelor.

De la „suntem conformi?" la „cât de bine ne guvernam datele?"

La zece ani de la intrarea în vigoare a GDPR, întrebarea care definește piața nu mai este daca o companie respecta regulile, ci cât de eficient își guverneaza datele. Pentru avocații specializați în aceasta arie, schimbarea se vede mai ales în modul în care companiile au ajuns sa înțeleaga importanța strategica a protecției și administrarii datelor. Mediul de afaceri privește astazi protecția datelor dintr-o perspectiva mult mai strategica, iar accentul a trecut de la conformarea formala la integrarea protecției datelor în mecanismele de guvernanța, de management al riscului și de transformare digitala.

„Daca în primii ani accentul era pus pe implementarea politicilor, registrelor și procedurilor interne, astazi organizațiile înțeleg ca datele reprezinta un activ strategic, iar administrarea lor are implicații directe asupra valorii companiei, reputației și rezilienței operaționale", a explicat Alexandra Nania, Managing Associate ZRVP. Pentru clienți, aceasta evoluție înseamna ca administrarea datelor a devenit o preocupare a conducerii executive, nu doar o responsabilitate a departamentului juridic.

Schimbarea se vede și în tipul de mandate pe care le gestioneaza firma. Proiectele tradiționale de audit și conformare ramân relevante, dar cele cu adevarat complexe vin din alta parte: incidente de securitate, investigații ale autorităților, proiecte de transformare digitala, implementarea soluțiilor bazate pe inteligența artificiala, transferuri internaționale de date și evaluari de due diligence în tranzacții. În mod particular, protecția datelor a

devenit o componenta relevanta a proceselor investiționale și a tranzacțiilor de fuziuni și achiziții. „Investitorii nu mai verifica doar existența documentației de conformare, ci urmaresc sa înțeleaga cât de matur este modelul de guvernanța a datelor și cât de bine sunt controlate riscurile digitale”, a aratat avocata. Istoricul incidentelor, relațiile cu furnizorii, transferurile internaționale, procesele de retenție și capacitatea organizației de a demonstra controlul asupra datelor au devenit elemente analizate constant în due diligence.

Cea mai importanta schimbare este însa una de mentalitate. „Daca în trecut întrebarea principala era «suntem conformi cu GDPR?», astazi discuția este mult mai strategica: «cât de bine ne guvernam datele și cât de pregatiți suntem sa gestionam riscurile generate de un ecosistem digital aflat într-o transformare permanenta?»”, a precizat Alexandra Nania. Întrebarea nu mai privește simpla respectare a unei norme, ci capacitatea companiei de a administra și controla un activ strategic. Protecția datelor nu mai este doar o cerința de conformare, ci o expresie a modului în care organizațiile își guverneaza datele, gestioneaza riscurile și construiesc încredere într-o economie tot mai dependenta de tehnologie și informație.

Multa vreme, presiunea de conformare a fost analizata în funcție de specificul sectorului de activitate. ZRVP observa ca reperul s-a schimbat: complexitatea nu mai este determinata exclusiv de industrie, ci de gradul de digitalizare și de intensitatea cu care o organizație folosește datele și tehnologia.

Exista, desigur, sectoare unde miza ramâne ridicata. Sanatatea este în continuare unul dintre cele mai sensibile domenii, din cauza volumului de date speciale și a nevoii de a echilibra protecția cu accesul rapid la informație și cu digitalizarea serviciilor medicale. În serviciile financiare, dificultatea vine din intersecția dintre protecția datelor, prevenirea fraudelor, cerințele de securitate și obligațiile de reglementare, iar pentru aceste organizații guvernanța datelor este deja o componenta centrala a managementului riscului. Sectorul tehnologic și operatorii de platforme se afla în centrul transformarilor legislative europene, fiindca pentru ei GDPR este doar una dintre piese, alaturi de AI Act, Data Act, DSA, DMA și NIS2; în consecința, analiza juridica depașește protecția datelor și atinge securitatea cibernetica, guvernanța digitala și responsabilitatea algoritmica.

„Observam o creștere semnificativa a complexității în sectoare precum retail, energie, real estate și resurse umane. Programele de fidelizare, marketingul personalizat, monitorizarea angajaților, recrutarea digitala și utilizarea instrumentelor AI genereaza astazi unele dintre cele mai sofisticate exerciții de analiza juridica și de evaluare a riscurilor”, a detaliat Managing Associate-ul ZRVP. În aceasta logica, riscul nu mai este dat de simpla apartenența la un sector, ci în felul concret în care fiecare companie lucreaza cu datele. „Astazi, diferențele dintre industrii sunt mai puțin relevante decât rolul pe care datele îl joaca în modelul operațional al fiecarei organizații”, a subliniat avocata.

Citește și

→ ZRVP, distinsa cu titlul de “Romania Patent Firm of the Year” la gala Managing IP Awards 2026 | De vorba cu Alina Tugearu (Partener) despre proprietatea intelectuala ca teren de strategie, prevenție și confruntare juridica în dosare cu miza ridicata: ”Am convingerea ca implicarea în unele dintre cele mai sofisticate și relevante dosare din piața a contribuit la recunoașterea de care ne bucuram azi”

Protecția datelor, parte dintr-o guvernanța mai larga

La un deceniu de la intrarea în vigoare a GDPR, protecția datelor nu mai poate fi tratata ca o arie autonoma de conformare. În viziunea practicii ZRVP, aceasta a devenit un pilon al guvernanței digitale, într-un cadru în care dimensiunile juridica, tehnologica, operațională și de risc sunt tot mai strâns interconectate.

Aceasta evoluție este accelerata de noile reglementari. Daca GDPR a obligat organizațiile sa își înțeleaga fluxurile de date și sa documenteze prelucrarile, NIS2 aduce în prim-plan reziliența operațională, gestionarea riscurilor cibernetice și capacitatea de raspuns la incidente. „În practica, cele doua dimensiuni sunt din ce în ce mai greu de separat", a observat Alexandra Nania. Conceptul de guvernanța a datelor a devenit central, iar administrarea lor nu mai poate ramâne doar la departamentele juridice sau de conformitate: cere implicarea managementului executiv și a funcțiilor de risc, securitate, IT și business.

În acest cadru se schimba și profilul avocatului. „Rolul avocatului specializat în protecția datelor a evoluat de la o funcție predominant orientata catre conformare la una cu o puternica dimensiune strategica", a spus avocata ZRVP. Valoarea adaugata nu mai vine exclusiv din interpretarea cadrului normativ, ci din capacitatea de a înțelege procesele de business, arhitectura tehnologica și riscurile utilizarii datelor. Concret, avocatul specializat este implicat tot mai devreme, înca din etapa în care opțiunile tehnologice și arhitectura deciziilor sunt în curs de definire.

♦ GDPR și AI Act, doua reglementari aflate într-o relație tot mai strânsa

Pentru tot mai multe organizații, GDPR nu mai reprezinta singurul reper relevant. În proiectele care integreaza inteligența artificiala, acesta trebuie analizat împreuna cu AI Act, întrucât cele doua reglementari abordeaza dimensiuni distincte ale aceleiași realitați tehnologice și organizaționale. GDPR stabilește regulile privind utilizarea datelor cu caracter personal, în timp ce AI Act introduce un cadru de guvernanța pentru dezvoltarea și folosirea sistemelor de inteligența artificiala.

„Pentru majoritatea organizațiilor, provocarea reala nu consta în aplicarea uneia dintre reglementari, ci în gestionarea simultana a ambelor", a explicat Alexandra Nania, Managing Associate ZRVP. Punctele cele mai sensibile țin de proveniența și calitatea datelor folosite la antrenarea sistemelor, de transparența fața de persoanele afectate, de profilare și de evaluarea impactului asupra drepturilor fundamentale. În practica, multe companii constata ca dificultatea nu ține de tehnologie în sine, ci de modul în care trebuie sa explice utilizarea acesteia și efectele pe care le produce. „Problema principala nu este tehnologia în sine, ci capacitatea de a explica și documenta modul în care aceasta funcționeaza", a aratat avocata. Cine valideaza datele folosite, cine verifica rezultatele, cine monitorizeaza riscurile și cine raspunde pentru deciziile luate cu sprijinul inteligenței artificiale sunt întrebarile care domina astazi agenda de conformare.

Raspunsul organizațiilor mature ia forma unor structuri interne de guvernanța a inteligenței artificiale, în care echipele juridice, de conformitate, securitate și tehnologie sunt implicate devreme. „Diferența dintre un proiect AI sustenabil și unul care genereaza expuneri semnificative nu este data de performanța algoritmilor, ci de existența unui cadru adecvat de control, documentare și responsabilizare", a punctat Managing Associate-ul ZRVP. Avantajul nu vine însa din viteza adoptarii. „Avantajul competitiv nu va aparține organizațiilor care adopta AI cel mai rapid, ci celor care reușesc sa implementeze tehnologia într-un cadru robust de guvernanța și gestionare a riscurilor", a adaugat avocata.

♦ Unde ramân în urma companiile din România

Întrebarea daca firmele românești sunt pregatite pentru guvernanța datelor în proiectele de inteligența artificiala nu

are un raspuns uniform. Nivelul de maturitate difera semnificativ de la o organizaţie la alta, însa ZRVP observa o tendinţa comuna: viteza cu care companiile adopta soluţii de inteligenţa artificiala depaşeşte adesea ritmul în care îşi dezvolta mecanismele interne de guvernanţa.

„În majoritatea proiectelor, provocarea nu este lipsa tehnologiei, ci lipsa vizibilitaţii asupra datelor şi proceselor care susţin utilizarea acesteia", a explicat Alexandra Nania. Multe organizaţii nu deţin înca o cartografiere completa a fluxurilor de date, nu au criterii clare pentru folosirea instrumentelor de inteligenţa artificiala şi nu au mecanisme formale de aprobare, monitorizare şi control. La acestea se adauga dificultatea de a evalua furnizorii şi de a înţelege cum funcţioneaza soluţiile implementate. Într-un mediu dominat de servicii furnizate de terţi, companiile trebuie sa înţeleaga nu doar condiţiile contractuale, ci şi implicaţiile privind utilizarea datelor, transferurile internaţionale şi distribuirea responsabilitaţilor.

Elementul care face diferenţa ramâne momentul implicarii juriştilor. „Cele mai reuşite proiecte sunt cele în care analiza juridica şi evaluarea riscurilor însoţesc procesul de implementare înca din fazele de proiectare, nu dupa ce tehnologia este deja operaţionala", a subliniat avocata ZRVP. Pe masura ce AI Act devine aplicabil etapizat, profesioniştii din domeniu anticipeaza ca guvernanţa inteligenţei artificiale va marca urmatoarea etapa de conformare pentru organizaţiile care şi-au consolidat deja programele de protecţie a datelor şi de securitate cibernetica.

Citeşte şi

→ Ghid pentru clienţii sofisticaţi | Cine domina arbitrajul comercial din România: avocaţii şi firmele recunoscute de Chambers, Legal 500, GAR 100 şi Lexology. Dr. Cosmin Vasile se detaşeaza ca „the leading star" pe piaţa locala, fiind descris de ghidurile internaţionale drept cel mai complet avocat de Dispute Resolution din România. ZRVP, TZA, NNDKP, Filip & Company şi PNSA au cele mai solide practici locale de arbitraj şi ar trebui sa fie primele alegeri ale firmelor care cauta sprijin în dispute guvernamentale şi corporative

---

Avocatul specializat în protecţia datelor, din expert în conformare în partener strategic

Practica protecţiei datelor traverseaza una dintre cele mai ample transformari ale ultimului deceniu, alimentata de extinderea şi suprapunerea tot mai accentuata a cadrului de reglementare. Daca în trecut GDPR era principalul reper, astazi organizaţiile trebuie sa se orienteze într-un ansamblu care include *AI Act, NIS2, Data Act, Digital Services Act* şi *Digital Markets Act*. „Aceste acte normative nu funcţioneaza izolat. Împreuna, ele definesc un nou model european de guvernanţa digitala, construit în jurul unor principii comune: responsabilitate, transparenţa, securitate şi control asupra datelor şi tehnologiilor utilizate", a aratat Alexandra Nania.

NIS2 este, în aceasta privinţa, un exemplu relevant. Pentru numeroase companii, obligaţiile privind gestionarea riscurilor cibernetice, continuitatea operaţionala şi raportarea incidentelor au ajuns sa aiba o importanţa comparabila cu cerinţele tradiţionale de protecţie a datelor. În acest nou cadru, conformarea nu mai poate fi abordata fragmentar, ci trebuie construita într-o logica unitara şi integrata.

Aceste evoluţii schimba, la rândul lor, aşteptarile faţa de avocat. Diferenţa nu mai este data exclusiv de cunoaşterea legislaţiei, ci şi de capacitatea de a înţelege modul în care tehnologia, datele şi procesele operaţionale susţin funcţionarea unei organizaţii. „Avocatul specializat în protecţia datelor nu mai este perceput doar ca un expert în conformare, ci ca un partener strategic în procesul de guvernanţa digitala", a precizat Managing

Associate-ul ZRVP. Rolul lui, a adaugat avocata, este sa traduca cerințele de reglementare în mecanisme sustenabile de control, responsabilitate și gestionare a riscurilor, aliniate obiectivelor de dezvoltare ale companiei. În acest nou rol, avocatul participa la fundamentarea deciziei de business, nu se limiteaza la validarea ei juridica.

♦ Cele mai grele dosare: când tehnologia trebuie explicata, nu doar folosita

Cele mai dificile probleme juridice din protecția datelor nu mai vin din interpretarea unei norme, ci din momentul în care complexitatea tehnologica întâlnește cerința de transparența și responsabilitate impusa de lege. ZRVP grupeaza aceste provocari în jurul câtorva puncte care revin în aproape orice proiect cu inteligența artificiala.

Primul ține de datele folosite la dezvoltarea și antrenarea sistemelor. „Organizațiile trebuie sa înțeleaga proveniența acestor date, baza legala care justifica utilizarea lor și riscurile asociate utilizarii unor seturi de date complexe, provenite din surse multiple", a explicat Alexandra Nania, Managing Associate ZRVP. Al doilea ține de profilare și de deciziile automatizate, care continua sa ridice întrebari sofisticate: companiile trebuie sa stabileasca daca sistemele produc efecte juridice sau afecteaza semnificativ persoanele și daca exista suficiente mecanisme de supraveghere și de intervenție umana.

Urmeaza explicabilitatea, devenita un test practic pe masura ce inteligența artificiala este folosita în procese critice de business. Organizațiile trebuie sa poata explica modul în care se genereaza un anumit rezultat sau o anumita recomandare. În fine, relația cu furnizorii de tehnologie capata o miza juridica directa. „Implementarea unei soluții dezvoltate de un terț nu transfera responsabilitatea juridica", a subliniat avocata. Practic, contractul cu furnizorul nu este o asigurare, iar controlul asupra riscului ramâne la organizație.

♦ Riscul nu vine dintr-un singur loc

Întrebata care sunt principalele surse de risc în proiectele de inteligența artificiala, avocata intervievata de ***Biz*** **Lawyer** arata ca acestea nu pot fi reduse la o singura cauza. „În practica, riscurile majore nu provin dintr-un singur factor, ci din suprapunerea mai multor vulnerabilități", a aratat Alexandra Nania.

Calitatea și proveniența datelor ramân printre cele mai importante surse de risc, fiindca performanța unui sistem depinde direct de datele pe care este construit, iar lipsa unei înțelegeri clare a sursei și a condițiilor de utilizare poate genera consecințe juridice și operaționale semnificative. La acestea se adauga dificultatea de a documenta baza legala pentru anumite utilizari și de a evalua impactul asupra persoanelor vizate, mai ales când sunt implicate date sensibile sau procese de profilare. Un risc des întâlnit ramâne tentația de a transfera raspunderea catre furnizorii de tehnologie. „În realitate, utilizatorul final ramâne responsabil pentru modul în care tehnologia este implementata și utilizata în cadrul organizației", a precizat avocata ZRVP.

În cele din urma, avocata reunește toate aceste observații într-o singura idee despre reziliența. „Cele mai reziliente organizații sunt cele care trateaza AI ca pe un exercițiu de guvernanța și control, nu exclusiv ca pe un proiect tehnologic", a spus Managing Associate-ul ZRVP. Astfel, discuția nu mai aparține departamentului tehnic, ci nivelului de decizie organizațională.

♦ Platformele digitale, în fața unui cadru de reglementare tot mai dens

Operatorii de platforme digitale și furnizorii de servicii online resimt cel mai acut presiunea noilor reglementari europene, într-un cadru în care protecția datelor reprezinta doar una dintre componentele unui ansamblu de obligații mult mai extins. „Pentru aceste organizații, GDPR reprezinta doar una dintre componentele unui cadru de

reglementare mult mai amplu, care include DSA, DMA, Data Act, AI Act şi NIS2", a explicat Alexandra Nania. Împreuna, aceste reguli schimba modul în care sunt proiectate, dezvoltate şi operate serviciile digitale.

Obligaţiile privind transparenţa, accesul la date, moderarea conţinutului, securitatea sistemelor, auditul algoritmilor şi gestionarea riscurilor devin parte din modelul operaţional al companiilor. În consecinţa, şi munca avocatului se schimba. „Analiza juridica nu mai este limitata la evaluari punctuale de conformitate, ci se extinde pe întreg fluxul de dezvoltare şi operare al iniţiativelor digitale, de la structurare şi implementare, pâna la monitorizare şi optimizare continua", a detaliat avocata. ZRVP observa deja o creştere a interesului pentru evaluarile de guvernanţa digitala, auditarea folosirii algoritmilor şi revizuirea relaţiilor cu furnizorii de tehnologie şi de servicii cloud.

Pentru aceste companii, conformarea îşi schimba natura. „Pentru platformele digitale, conformarea nu mai este un proiect cu un termen de finalizare. A devenit o funcţie permanenta a modelului de business", a punctat Managing Associate-ul ZRVP. În consecinţa, resursele financiare şi atenţia alocate conformarii nu mai au un caracter punctual, ci devin o componenta permanenta a operaţiunilor curente.

Citeşte şi

→ Practica de Energie & Resurse Naturale de la ZRVP este construita pe mandate transfrontaliere, expertiza sectoriala profunda şi o echipa cu vizibilitate internaţionala | De vorba cu Lidia Trandafir (Managing Associate) despre dinamica şi perspectivele unei pieţe în plina ascensiune, în care fotovoltaicul ramâne locomotiva investiţiilor, stocarea câştiga rapid teren, iar hidrogenul şi e-fuels se contureaza la orizont ca frontiera urmatorului ciclu de creştere

---

Cum arata, în practica, o guvernanţa matura a datelor

Întrebarea care urmeaza firesc este cum ar trebui sa arate o guvernanţa matura a datelor într-o companie care lucreaza într-un mediu digital complex. Avocata ZRVP îşi construieşte raspunsul pornind de la respingerea a doua abordari simplificatoare frecvent întâlnite. „O guvernanţa matura a datelor nu este construita în jurul unui singur departament şi nici nu se reduce la existenţa unor politici interne", a explicat Alexandra Nania.

Modelele care funcţioneaza sunt cele în care responsabilitaţile sunt clar distribuite între funcţiile juridice, conformitate, IT, securitate cibernetica, managementul riscului şi conducerea executiva, într-un cadru integrat de decizie. O astfel de abordare presupune politici coerente privind utilizarea şi clasificarea datelor, retenţia, controlul accesului, folosirea inteligenţei artificiale, gestionarea furnizorilor şi raspunsul la incidente, dar şi mecanisme de monitorizare, audit şi îmbunataţire continua. Un rol central revine conducerii executive. „Mesajul transmis de GDPR, NIS2 şi AI Act este convergent: responsabilitatea pentru guvernanţa datelor şi a tehnologiei nu poate fi fragmentata sau externalizata exclusiv catre funcţiile tehnice ori juridice, ci trebuie asumata la nivel organizaţional", a aratat avocata.

Testul final al maturitaţii nu sta în volumul documentaţiei. „Maturitatea nu este definita de volumul documentaţiei interne, ci de capacitatea organizaţiei de a demonstra ca aceste mecanisme sunt implementate, funcţionale şi integrate în mod real în activitatea curenta", a subliniat Managing Associate-ul ZRVP. În practica, un set amplu de politici nu poate substitui dovada aplicarii lor efective.

♦ Ce cauta acum autoritățile

Autoritățile fac aceeași trecere de la forma la fond atunci când verifica firmele. „Investigațiile nu mai urmaresc exclusiv existența unor politici sau registre interne. Accentul se muta asupra capacității organizației de a demonstra ca mecanismele de control funcționeaza efectiv și ca deciziile relevante sunt documentate și justificabile”, a explicat Alexandra Nania. Trasabilitatea proceselor și documentarea evaluarilor de risc devin elemente esențiale în orice control.

În paralel, incidentele de securitate continua sa genereze unele dintre cele mai sensibile exerciții juridice, în care organizațiile trebuie sa evalueze rapid obligațiile de notificare, impactul asupra persoanelor vizate și masurile de limitare a consecințelor. Vulnerabilitățile întâlnite cel mai des in practica sunt previzibile, dar persistente: documentația incompleta, justificarea insuficienta a unor decizii, relațiile insuficient reglementate cu furnizorii și dificultatea de a demonstra masurile aplicate efectiv.

Concluzia ZRVP redefinește ideea de reziliență. „Diferența dintre vulnerabilitate și reziliența organizațională nu este definita de absența incidentelor, ci de capacitatea de a raspunde într-un mod structurat, documentat și proporțional, care poate fi susținut în fața verificarilor interne și externe”, a precizat avocata. Pentru companii, asta înseamna ca obiectivul realist nu este eliminarea oricarui incident, ci pregatirea pentru a-l gestiona corect.

Urmatorul deceniu: de la implementarea GDPR la guvernanța digitala

Privind spre urmatorii trei-cinci ani, avocata ZRVP identifica o direcție majora, în care converg toate celelalte evoluții: consolidarea guvernanței digitale. Inteligența artificiala, securitatea cibernetica, reziliența operațională, transferurile internaționale de date și responsabilitatea folosirii tehnologiilor emergente vor redefini agenda juridica a organizațiilor și vor genera mandate aflate la intersecția dintre reglementare, tehnologie și managementul riscului.

„Vom vedea tot mai multe proiecte aflate la intersecția dintre GDPR, AI Act și NIS2, unde provocarile juridice nu vor putea fi separate de aspectele tehnologice și operaționale”, a aratat Alexandra Nania. În paralel cu creșterea nivelului de reglementare, practica anticipeaza o cerere tot mai mare pentru modele eficiente de guvernanța și de simplificare operațională, care sa permita conformarea fara a afecta agilitatea și competitivitatea companiilor. Implementarea sistemelor de inteligența artificiala, raspunsul la incidente complexe, proiectele de transformare digitala, evaluarile de due diligence tehnologic și restructurarea modelelor de guvernanța vor cere echipe multidisciplinare, iar valoarea avocatului va fi data, din nou, mai puțin de interpretarea legislației și mai ales de capacitatea de a o transpune în soluții concrete și aplicabile.

Linia de fond este, pentru Managing Associate-ul ZRVP, o schimbare de etapa. „Daca ultimul deceniu a fost despre implementarea GDPR, urmatorul va fi despre integrarea protecției datelor într-un model mai amplu de guvernanța a tehnologiei și a riscurilor digitale”, a spus avocata. Într-o economie tot mai dependenta de tehnologie, a adaugat ea, încrederea, transparența și reziliența ajung sa conteze la fel de mult ca inovația, iar avantajul va aparține organizațiilor care construiesc din timp mecanisme de guvernanța și control, în loc sa reacționeze la fiecare noua reglementare.

Citește și

→ ZRVP, desemnata din nou „Firma de Avocatura a Anului din România” la Lexology Index Awards 2025 | Dr. Cosmin Vasile (Managing Partner): Un premiu obținut doi ani la rând spune un lucru simplu:

ca echipa merge în direcţia buna. O astfel de recunoaştere confirma nivelul profesional atins şi, în acelaşi timp, ne obliga sa ramânem la fel de exigenţi

---

Recunoașterea ZRVP în zona IP & TMT și protecția datelor

În directoarele internaționale, poziționarea *Zamfirescu Racoți Vasile & Partners* în aceasta arie este reflectata prin practica de proprietate intelectuala, tehnologie, media și telecomunicații, în absența unei secțiuni distincte dedicate protecției datelor. Recunoașterea relevanta pentru aceasta arie se regasește, așadar, în practica de IP & TMT, unde conformarea, contractele privind prelucrarea datelor și cerințele de securitate se întâlnesc în mod natural cu dreptul tehnologiei.

În Legal 500 EMEA, ediția curenta, ZRVP este clasata în *Tier 2* la *Intellectual Property* - România. Este o poziție solida și stabila, care confirma greutatea firmei în litigiile de proprietate intelectuala, în special în litigiile de brevete. În același clasament, firma ocupa *Tier 1* la trei capitole de tradiție, *Dispute Resolution, Restructuring and Insolvency* și *White-collar Crime*, ceea ce arata profilul ei general de forța în zona contencioasa și de afaceri.

În Chambers Europe, ediția 2026, ZRVP este clasata în *Band 3* la *Intellectual Property & TMT* în România, o prezența constanta, menținuta de șapte ani consecutivi. În descrierea ghidului, echipa este cunoscuta pentru litigiile de brevete în beneficiul clienților din sectorul farmaceutic și energetic, precum și pentru anularea și contrafacerea de desene și marci și pentru chestiunile de drept de autor. Coordonatoarea practicii de proprietate intelectuala este avocata **Alina Tugearu**, apreciata pentru expertiza în disputele de brevete și în anularea marcilor.

Tot în Chambers sunt publicate doua testimoniale de la clienți, ambele privind practica de proprietate intelectuala. Primul reține ca „*echipa cunoaște foarte bine atât dreptul român, cât și problemele de drept european legate de proprietatea intelectuala*”. Al doilea adauga ca „*avocații au un simț comercial foarte bun atunci când abordeaza disputele dintr-o perspectiva de afaceri*”.

La nivel de firma, ZRVP a primit recunoașteri suplimentare care întaresc acest profil: titlul *„Romania Firm of the Year” la Lexology Index* în 2024 și 2025 și premiul *Managing IP Firm of the Year pentru litigii de brevete în 2025*. Pe scurt, recunoașterea firmei în aceasta zona se reflecta prin practica de IP & TMT, Tier 2 la Legal 500 și Band 3 la Chambers Europe 2026, și prin reputația ei generala în zona contencioasa. Practica de protecția datelor și securitate cibernetica, dezvoltata în cadrul echipei de consultanța, se sprijina pe aceasta recunoaștere de ansamblu.