



## Studiu de caz: Audit high level GDPR

Client: Ropharma  
Verticală: healthcare

### Ropharma se aliază la cerințele GDPR cu ajutorul consultanților NOD

Intrarea în vigoare a noului Regulament general pentru protecția datelor cu caracter personal obligă companiile să își reaseze procesele și procedurile interne și să adopte măsuri extinse de securitate. Pentru a se alinia noilor cerințe, Grupul Ropharma a accesat pachetul de servicii de consultanță „Audit GDPR high-level”, creat și dezvoltat de NOD și Casa de Avocatură Dan Mihai. În urma procesului de audit – care a durat jumătate din timpul necesar grupului pentru a-l realiza cu resurse interne – Ropharma a stabilit și priorizat o serie de măsuri și soluții concrete pentru conformitatea cu normativele GDPR, a crescut disponibilitatea și securitatea datelor și aplicațiilor și a optimizat utilizarea resurselor IT la nivelul întregului grup.

### Despre client

Grupul Ropharma s-a impus în ultimii 10 ani ca un jucător important pe piața serviciilor medicale din România. Grupul deține propriile fabrici de medicamente, suplimente alimentare și lapte praf, având 50 de produse în portofoliu la care adaugă anual 5-7 produse noi. Cu 6 depozite la nivel național deservite de propria flotă auto și cu o rețea de 143 de farmacii aflată în extindere constantă, grupul ocupă un loc de frunte și în ierarhia distribuitorilor de produse farmaceutice, parafarmaceutice și dermatocosmetice.

Nu în ultimul rând, Ropharma este acționar majoritar al Spitalului multidisciplinar Sf. Constantin, din Brașov. Cotat ca fiind una dintre cele mai curate instituții medicale din Europa (premiată în cadrul campaniei globale a Organizației Mondiale a Sănătății pentru siguranța pacientului „Clean care is safer care”), spitalul este totodată și primul centru privat de chirurgie robotică din România, robotul DaVinci fiind instalat în martie 2017.

### Situația inițială: imperativul GDPR

Adoptarea la nivelul Uniunii Europene a noului Regulament general pentru protecția datelor cu caracter personal (mai 2016) și obligativitatea alinierii țărilor membre la cerințele acestuia începând cu 25 mai 2018 a reprezentat o preocupare prioritară pentru managementul Ropharma încă de anul trecut.

Grupul a început din primăvara lui 2017 să analizeze implicațiile GDPR (General Data Protection Regulation) în zona serviciilor medicale furnizate prin intermediul Spitalului Sf. Constantin, precum și la nivelul lanțului de farmacii. În cadrul spitalului, funcționează un serviciu de programări – operat prin intermediul Call Center-ului propriu – care colectează, stochează și procesează date cu caracter personal ale persoanelor tratate în regim ambulatoriu, operațiuni sensibile din punct de vedere date personale.

Pe de altă parte, la nivelul farmaciilor Ropharma funcționează mai multe programe de fidelizare și promovare

derulate de către departamentele de marketing ale grupului, prin intermediul cărora clienților li se oferă o serie de reduceri (pe baza unui sistem propriu de punctaj). Gestionarea campaniilor de marketing și a datelor pacienților se realizează prin aplicații dedicate, dezvoltate in-house, integrate cu soluțiile de retail. Și aceste operațiuni sunt reglementate însă de către normativele GDPR.

„Pentru că, în cazul nostru, clientul este atât în interior – avem peste 1.100 de angajați în lanțul de farmacii și aproximativ 200 la spital –, cât și în afară, ne-am dorit să reasezăm și redefinim sistemul de proceduri interne pentru a ne alinia toate procesele la cerințele noului regulament”, explică **Ciprian Băcanu, IT Project Manager Ropharma.**

### Identificarea partenerilor

Pentru atingerea acestor obiective, Ropharma a inițiat în mai 2017 o etapă de analiză a ofertelor. În urma acestui proces, grupul a selectat firma Ask4IT, partener tehnologic al Network One Distribution (NOD), furnizor național de soluții, echipamente și servicii IT.

Prin intermediul Ask4IT, Ropharma a accesat pachetul de servicii de consultanță „Audit GDPR high-level”, creat și dezvoltat de către NOD în colaborare cu Casa de Avocatură Mihai&Co Business Lawyers și lansat pe piață la finalul trimestrului trei 2017. Pachetul de Auditare High Level – face parte dintr-o suită de servicii ce susțin implementarea și conformitatea GDPR

compusa din servicii de cartografiere a datelor, training pentru angajați, personalizare și implementare proceduri GDPR, pregătirea și suportul pentru DPO (Data Protection Officer) „IT & Cybersecurity Audit” (evaluare a nivelului de securitate, recomandări pentru remedierea problemelor și îmbunătățirea nivelului de protecție, training-uri etc.) și „Software Asset Management” (inventariere a mijloacelor software, optimizare a modalităților de licențiere și a costurilor software, training-uri pentru utilizatori și administratori de sistem etc.)

„Ask4IT este un partener mai vechi al grupului Ropharma pe zona serviciilor IT de suport și externalizare și a acționat ca un garant al pachetului de consultanță oferit de NOD și Casa de Avocatură. Alegerea a fost decisă atât de vechimea relației existente și de reputația bună pe care o au cele trei companii în piață, cât și de faptul că partenerii Ask4IT au competențe avansate pe zona tehnică și experiență în zona serviciilor medicale și farma, fapt care ne-a ajutat să obținem răspunsuri concrete la cerințele noastre specifice”, precizează IT Project Managerul Ropharma.

## Derularea proiectului

În faza preliminară a proiectului au avut loc mai multe întâlniri de definire și detalieri ale obiectivelor și etapelor proiectului în care au fost stabiliți pașii concreți care trebuie urmați în cadrul procesului de audit.

Procesul a demarat efectiv printr-un workshop/seminar la care au participat factorii decidenți din cadrul companiilor Ropharma implicate: directori ai departamentelor de marketing, IT, juridic, HR etc. Seminarul s-a axat pe prezentarea și discutarea noilor reglementări introduse de către GDPR și analiza impactului pe care acestea le pot avea asupra proceselor interne ale companiilor din grup.

În cadrul workshop-ului, la care au participat circa 30 de persoane-cheie din companiile implicate, au fost colectate informații despre modul în care sunt preluate, stocate și prelucrate datele, cum sunt transmise acestea, cum este obținut consimțământul clienților, care sunt măsurile recomandate de minimizare a datelor etc.

Pe baza acestor informații, NOD și

partenerii săi au creat un chestionar extins, care a adresat două direcții de bază: aspectele legate de zona juridică și procedurală a companiei și cele aferente zonei IT, cu elementele specifice.

Rezultatele chestionarelor – agregate și analizate – au servit ca bază pentru generarea raportului de audit, care a dat o imagine de ansamblu asupra stadiului în care se afla grupul Ropharma la acel moment în raport cu cerințele Regulamentului general pentru protecția datelor cu caracter personal și a oferit o serie de recomandări concrete pentru atingerea obiectivelor stabilite. Raportul a fost prezentat top-managementului companiilor din grup, fiind detaliate rezultatele obținute și măsurile specifice recomandate.

## Rezultatele obținute

Raportul realizat de către NOD și Casa de Avocatură Mihai&Co Business Lawyers a evidențiat o serie de aspecte care trebuie ameliorate la nivel procedural și juridic în cadrul grupului Ropharma, precum și măsuri de diminuare a riscurilor informatice, recomandările fiind prioritizate pe mai multe niveluri.

Rezultatele raportului au fost asumate de către companiile din cadrul grupului, care s-au angajat în abordarea tuturor măsurilor de optimizare recomandate pentru atingerea nivelului dorit de conformitate cu cerințele GDPR.

Astfel, raportul a asigurat, în principal, o definire a principalelor categorii de date care sunt colectate, procesate și stocate de către companiile Ropharma, duratele de păstrare, procedurile de anonimizare și cele de ștergere, stabilind modalitățile concrete prin care se realizează aceste procese. Prin suprapunerea rezultatelor chestionarelor cu cerințele GDPR, consultanții au identificat o serie de măsuri imediate, capabile să asigure minimizarea datelor (eliminarea colectării informațiilor care nu sunt necesare, reducerea numărului de depozite de date etc.), precum și modalități clare de solicitare, obținere și retragere a consimțământului pacienților și clienților.

Raportul a facilitat și stabilirea de noi modalități de lucru cu companiile împuternicite să deruleze relații cu clienții Ropharma. Pe baza acestor proceduri au fost create deja o serie de recomandări către terți, pentru ca

aceștia să își poată reajusta politicile de lucru cu clienții, în conformitate cu cerințele GDPR și Ropharma, precum și acte adiționale la contracte, prin care se asigură securitatea, integritatea și disponibilitatea datelor și după încetarea relațiilor contractuale.

Pe zona de HR au fost identificate o serie de măsuri practice de optimizare a relației cu angajații, realizându-se o împropiatare a normelor, fiecare proces fiind documentat și justificat legal. De asemenea, au fost create proceduri de informare, instruire și conștientizare adresate cu precădere angajaților care sunt implicați direct în prelucrarea datelor cu caracter personal. Totodată, au fost identificate mai multe soluții de monitorizare, utilizate deja, care pot extinde vizibilitatea asupra activităților desfășurate și minimiza riscul pierderilor de date. Pentru a securiza accesarea datelor din exteriorul companiilor Ropharma și a reduce la minimum riscurile de acces neautorizat s-a implementat și o aplicație autentificare multifactor, cu certificat digital, conformă cu cerințele GDPR.

În urma Raportului de audit, Ropharma a numit și responsabilii cu protecția datelor cu caracter personal (Data Protection Officer - DPO), în cadrul entităților din grup, unde această funcție era necesară.

Întregul proces de audit derulat de către NOD și partenerii săi a durat trei luni, jumătate din timpul care i-ar fi fost necesar grupului Ropharma pentru a-l realiza cu resurse interne. Rezultatul final, Raportul de audit GDPR, este un produs complex care a permis grupului să cunoască și înțeleagă nivelul de conformitate cu cerințele regulamentului, să își prioritizeze investițiile și eforturile și să definească măsuri concrete de răspuns la potențialele incidente.

„Efectele raportului de audit realizat în cadrul Ropharma depășesc cerințele GDPR pentru că rezultatele acestuia ne ajută efectiv să ne îmbunătățim activitatea pe mai multe direcții și ne-au condus către obținerea unui plus de performanță în alocarea resurselor. Totodată, am obținut o eficientizare a modului în care este utilizat IT-ul la nivelul întregului grup și ne-am îmbunătățit substanțial nivelul de disponibilitate și securitate”, a concluzionat Ciprian Băcanu.

“

„Alinierea la cerințele Regulamentului general de protecție a datelor cu caracter personal nu este un obiectiv finit în timp, ci reprezintă un proces evolutiv, asupra căruia revenim permanent în cadrul grupului Ropharma.”

Ciprian Băcanu, IT Project Manager Ropharma

”

“

„Colaborarea cu NOD ne-a consolidat relația cu Ropharma și ne-a deschis multiple oportunități de afaceri. Pachetul de servicii GDPR este foarte competitiv, atât financiar cât și ca structură, ceea ce contează în relațiile cu piața companiilor mici și medii. Partenerii implicați au niveluri ridicate de competență și experiență, iar abordarea comună juridică și tehnică aduce clientului o valoare adăugată mare. Pentru noi, auditul GDPR devine punctul de plecare pentru implementarea unor noi tehnologii.”

Eduard Galan, Director General AskForIT

”

“

„Suntem o casă de avocatură specializată pe relații business-to-business, prin urmare subiectul GDPR a fost în atenția noastră de la început. Împreună cu NOD am dezvoltat pachetul de servicii «High Level Audit», cu o abordare multidisciplinară, gândit pe principiul implementării unui sistem informatic. Pachetul răspunde necesităților clientului de a implementa noul regulament, atât din punct de vedere al procedurilor, dar mai ales din perspectiva conformității operaționale. Astfel, ne-am focalizat asupra urmării proceselor de business și alinierii la reglementările GDPR cât mai aproape de procesele de business ale clientului, recomandându-i, acolo unde a fost cazul, ajustări și corecții. De asemenea, ne-am concentrat și pe instruirea angajaților care intră în contact cu datele personale și am încercat să le descriem și să le explicăm noua reglementare astfel încât aceasta să fie acceptată și să fie cât mai ușor de urmărit și aplicat de aceștia în activitatea de zi cu zi. Dacă tematica GDPR este abordată dintr-o perspectivă «business driven» poate constitui o bună oportunitate pentru companii de consolidare a procesele de business și, implicit, de creștere a competitivității. Împreună cu NOD am încercat să urmărim acest deziderat și să cream parteneriate cu clienții pentru care am implementat pachetul «High Level Audit».”

Dan Mihai, Casa de Avocatură Mihai&Co Business Lawyers

”

“

„Noul Regulament general pentru protecția datelor cu caracter personal va genera, în timp, o reorganizare a tuturor proceselor interne pe care companiile le desfășoară. Pachetul de servicii de consultanță «GDPR High Level Audit» dezvoltat în cadrul NOD și cu ajutorul partenerilor noștri este special conceput și calibrat pentru a răspunde nevoilor clienților noștri de aliniere la cerințele GDPR. Este o abordare logică, care pune pe primul loc consultanța, urmată de livrarea de soluții și apoi de implementarea acestora. Furnizăm în permanență soluții alinate la cele mai noi tehnologii, care asigură companiilor un mediu de lucru mai sigur, orientat către creșterea performanțelor, precum și optimizarea costurilor pe termen mediu și lung printr-un randament superior al investiției.”

Bogdan Lupu, Microsoft Lead, Network One Distribution

”