CONFERINȚA STABRIS

GDPR: preocupări, probleme, soluții“

Iași, 17 iulie 2018

STABRIS

Consultanța pentru conformitatea la GDPR – abordări și rezultate

Cristian OBREJA

Ce este consultanța în management?

Este un ansamblu de activități realizate în scopul identificării și investigării problemelor unei organizații și/sau oportunităților de care poate beneficia aceasta, care se finalizează prin recomandarea unor acțiuni corespunzătoare și asistență la implementarea acestor recomandări.

Sursa: http://www.finantare.ro/biblioteca/2011/Studiu-managementul-firmelor-de-consultanta-finantarero.pdf

În ce constă consultanța pentru conformitatea la RGPD?

- în *identificarea* și *investigarea* problemelor unei organizații din punct de vedere a respectării prevederilor Regulamentului și
- *emiterea* unor recomandări care, dacă sunt puse în aplicare, vor avea ca efect, **într-un anumit interval de timp**, conformitatea cu cerințele RGPD.

Pe ce fond au apărut solicitările de consultanță pentru asigurarea conformității cu RGPD?

Atenția tuturor organizațiilor a fost atrasă de nivelul foarte ridicat al amenzilor prevăzute de Regulament: până la **10 – 20 milioane de euro sau între 2% și 4% din cifra de afaceri la nivel internațional**.

La nivel național, pe fondul apariției publice a unor puncte de vedere extreme referitoare la problematica implementării RGPD, conducerile organizațiilor care prelucrau date cu caracter personal, au început să fie preocupate de noua perspectivă a continuării relaționării cu clienții persoane fizice, care se părea că va fi dominată de probleme.

Exemplu: În luna februarie 2018, reprezentantul unei case de avocatură declara că, în contextul generat de aplicarea GDPR, va urma un „nou val de procese colective împotriva firmelor mari care au clienți persoane fizice“ și că Regulamentul a dus la „conturarea unei noi arii de practică în materia litigiilor“.
Sursa: https://www.startupcafe.ro/afaceri/gdpr-proces-firma-despagubiri.htm

Cum acționează managementul organizațiilor pentru a asigura conformitatea cu RPGD?

Regulamentul este un document complex, mai ales prima parte în care sunt expuse cele 173 de motive (considerente), pe care persoanele fără o pregătire de specialitate, în special în domeniile juridic și IT, îl parcurg și îl înțeleg cu greutate.

Documentele postate pe site-ul ANSPDCP, în special Ghidul orientativ de aplicare a RGPD destinat operatorilor, au un format mai prietenos și pot fi studiate cu ușurință de către orice persoană interesată.

După parcurgerea acestora, pentru managementul unei organizații, **începe să se prefigureze identificarea unei soluții**.

Managementul organizației – încercarea identificării unei soluții (1)

PRINCIPALELE OBLIGAŢII PENTRU OPERATORII DE DATE ÎN APLICAREA RGPD

DESEMNAREA UNUI RESPONSABIL CU PROTECŢIA DATELOR

Pentru a îndruma modul în care sunt gestionate datele cu caracter personal în cadrul unui operator sau al unei persoane împuternicite de operator, în anumite situaţii, este necesară o persoană care să exercite o misiune de informare, de consiliere și de control în plan intern: **responsabilul cu protecţia datelor**.

Chiar dacă entitatea nu are obligaţia expresă de a desemna un responsabil cu protecţia datelor, ANSPDCP recomandă numirea acestuia, în considerarea efectului benefic al activităţii responsabilului în vederea asigurării respectării Regulamentului General de Protecţia Datelor de către operatorul respectiv sau persoana împuternicită de operator.

Un **responsabil cu protecţia datelor** reprezintă un avantaj major pentru operator în vederea înţelegerii şi respectării obligaţiilor prevăzute de RGPD, dialogului cu autorităţile pentru protecţia datelor şi reducerii riscurilor apariţiei unor litigii.

Rolul responsabilului cu protecţia datelor

- **să informeze și să consilieze** operatorul sau persoana împuternicită de operator, precum și angajaţii acestora cu privire la obligaţiile existente în domeniul protecţiei datelor cu caracter personal;
- **să monitorizeze respectarea RGPD** și a legislaţiei naţionale în domeniul protecţiei datelor;
- **să consilieze operatorul sau persoana împuternicită** în legătură cu realizarea de studii de impact privind protecţia datelor și să verifice efectuarea acestora;
- **să coopereze cu autoritatea pentru protecţia datelor** și să reprezinte punctul de contact în relaţia cu aceasta.

ANS

Managementul organizației – încercarea identificării unei soluții (2)

PRIORITIZAREA ACŢIUNILOR DE ÎNTREPRINS

Operatorul și persoana împuternicită de operator **identifică acţiunile** care trebuie întreprinse pentru conformarea la cerinţele impuse de RGPD.

Se **prioritizează** aceste acţiuni în funcţie de riscurile pe care le prezintă prelucrările efectuate pentru drepturile și libertăţile persoanelor vizate.

După identificarea prelucrărilor de date cu caracter personal efectuate în cadrul entităţii, se stabilesc, pentru fiecare dintre acestea, acţiunile care trebuie întreprinse în vederea respectării obligaţiilor impuse de Regulamentul General privind Protecţia Datelor.

Indiferent de prelucrările efectuate, se vor avea în vedere, în principal, următoarele aspecte:

- colectarea și prelucrarea **doar a datelor strict necesare** pentru realizarea scopurilor;
- identificarea **temeiului legal** în baza căruia se efectuează prelucrarea raportat la art. 6 din Regulamentul General privind Protecţia Datelor (ex. consimţământul persoanelor vizate, contract, obligaţie legală);
- revizuirea/completarea **informaţiilor furnizate persoanelor vizate**, astfel încât să respecte cerinţele impuse de Regulamentul General privind Protecţia Datelor (articolele 12, 13 și 14);
- asigurarea că **persoanele împuternicite** își cunosc noile obligaţii și responsabilităţi;
- verificarea existenţei clauzelor contractuale și actualizarea obligaţiilor **persoanelor împuternicite** privind securitatea, confidenţialitatea și protecţia datelor cu caracter personal prelucrate;
- stabilirea modalităţilor de exercitare a **drepturilor persoanelor vizate** (ex. dreptul de acces, dreptul de rectificare, dreptul la portabilitate, retragerea consimţământului);
- verificarea **măsurilor de securitate** implementate.

Managementul organizației – încercarea identificării unei soluții (3)

Se pot aplica **măsuri speciale,** precum: evaluarea impactului asupra protecţiei datelor, extinderea dreptului la informare al persoanelor vizate, obţinerea consimţământului persoanelor vizate (după caz), obţinerea autorizării pentru transferurile de date în state terţe (dacă este cazul), în cazul în care prelucrările de date cu caracter personal efectuate în cadrul operatorului sau persoanei împuternicite de operator îndeplinesc următoarele **caracteristici**:

- Prelucrarea efectuată vizează și categorii de date precum:
  - date care dezvăluie originea rasială sau etnică, opiniile politice, filozofice sau religioase, apartenenţa sindicală;
  - date privind sănătatea sau orientarea sexuală, date genetice sau biometrice;
  - date referitoare la infracţiuni sau condamnări penale;
  - date referitoare la minori.

- Prelucrarea efectuată are ca scop și ca efect:
  - monitorizarea permanentă pe scară largă a unei zone accesibile publicului;
  - evaluarea sistematică și aprofundată a unor aspecte personale, inclusiv profilarea, pe baza căreia sunt luate decizii care produc efecte juridice referitoare la o persoană fizică sau care o afectează pe aceasta în mod semnificativ.

- Prelucrarea efectuată implică transferuri de date în afara Uniunii Europene, către state care nu asigură un nivel de protecţie adecvat recunoscut de Comisia Europeană.

Se realizează o analiză aprofundată a legislației privind protecţia datelor și a cerinţelor impuse de Regulamentul General privind Protecţia Datelor pentru a stabili măsurile care trebuie aplicate la nivelul fiecărui operator, în funcţie de sectorul de activitate și specificul prelucrării/prelucrărilor efectuate.

Managementul organizației – încercarea identificării unei soluții (4)

GESTIONAREA RISCURILOR

În cazul în care au fost identificate prelucrări de date cu caracter personal susceptibile de a prezenta **riscuri ridicate** pentru drepturile şi libertăţile persoanelor fizice, operatorul va efectua o **evaluare a impactului asupra protecţiei datelor**, în condiţiile art. 35 din Regulamentul General privind Protecţia Datelor.

Evaluarea impactului asupra protecţiei datelor se realizează **anterior colectării** datelor cu caracter personal și efectuării prelucrării.

Se va pune accent pe **estimarea riscurilor asupra protecţiei datelor din punctul de vedere al persoanelor vizate, luând în considerare natura datelor, domeniul de aplicare, contextul și scopurile prelucrării și utilizarea noilor tehnologii**.

Managementul organizației – încercarea identificării unei soluții (5)

ORGANIZAREA PROCEDURILOR INTERNE

Pentru a asigura permanent un nivel ridicat de protecţie a datelor cu caracter personal, operatorul trebuie să elaboreze proceduri interne care să garanteze respectarea protecţiei datelor în orice moment, luând în considerare toate evenimentele care pot apărea pe parcursul efectuării prelucrărilor de date, precum:

- breșe de securitate;
- solicitări privind exercitarea drepturilor persoanelor vizate;
- modificarea datelor cu caracter personal colectate;
- schimbarea prestatorului.

Ce acțiuni au întreprins inițial mulți dintre conducătorii organizațiilor? (1)

Prima tendință a managementului și, desigur, cea mai eficientă din punct de vedere financiar, a fost de a încerca să asigure conformarea prin resurse umane proprii.

La multe dintre organizații, managementul a considerat că poate rezolva problema prin desemnarea unui Responsabil cu protecția datelor cu caracter personal (DPO) și prin trimiterea acestuia la un curs de specialitate.

Ce acțiuni au întreprins inițial mulți dintre conducătorii organizațiilor? (2)

În multe cazuri, pe fondul necunoașterii prevederilor RGPD, persoana care a urmat cursul de DPO se afla în incompatibilitate cu ocuparea unei astfel de funcții.

„Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.“ – *art. 38, alin. 6 din RGPD*

Ce acțiuni au întreprins inițial mulți dintre conducătorii organizațiilor? (3)

”Ca regulă generală, funcții din cadrul organizației cu care poate intra în conflict pot include funcții de conducere (cum ar fi **director executiv**, **director operațional**, **director financiar**, **șeful serviciului medical**, **șeful departamentului de marketing**, **șef departamentului de resurse umane** sau **șeful departamentului IT**), dar, în același timp, și **alte funcții inferioare dacă acestea conduc la posibilitatea de a stabili scopurile și mijloacelor de prelucrare**. În plus, un conflict de interese poate apărea, de asemenea, de exemplu, în situația în care un DPO extern este rugat să reprezinte operatorul sau persoana împuternicită de operator în instanță, în cazurile care implică probleme de protecție a datelor.”

Ghidul privind Responsabilul cu protecția datelor
http://www.dataprotection.ro/servlet/ViewDocument?id=1384

Utilitatea cursului de Responsabil protecția datelor cu caracter personal (DPO)

Persoanele care au parcurs cursul DPO, au primit un volum important de informații care cuprindeau, pe lângă prevederile RGPD, și aspecte referitoare la:

- precizările practice ale Ghidurilor întocmite de Grupul de lucru 29
- punctele de vedere exprimate de ANSPDCP pe diverse teme/problematici de interes
- exemple întâlnite în practică, cu ocazia realizării unor activități de consultanță RGPD la firme din diverse domenii de activitate
- prezentarea/explicarea unor soluții tehnice – cerințe care trebuie incluse în caietele de sarcini întocmite în scopul achiziționării unor soluții informatice care să sprijine organizația în procesul de asigurare a conformității cu RGPD.

Cei mai mulți dintre cursanți au fost foarte activi și au pus întrebări cu caracter aplicativ pe linia implementării prevederilor RGPD în organizațiile din care proveneau. Ulterior, o parte au menținut legătura cu firma STABRIS și au solicitat sprijin pentru realizarea unor documente specifice RGPD.

Cum s-a acționat ulterior la nivelul organizațiilor pentru asigurarea conformității cu GDPR?

<u>Soluția 1:</u> Utilizarea resursei umane și tehnice proprii pentru parcurgerea etapelor precizate în Ghidul orientativ destinat operatorilor.

Această soluție a fost adoptată în special de organizațiile mari de stat (administrație publică, universități, spitale etc.) care dispuneau de resursă umană calificată (securitate organizațională, juridic, IT etc.) către care puteau redistribui noile sarcini (prin cumul) cu costuri nesemnificative.

<u>Soluția 2: Încheierea unor contracte cu firme de consultanță specializate</u>

Această abordare a aparținut în general firmelor cu o cifră de afaceri mare, care dispuneau de resursele financiare achiziționării serviciilor de consultanță, fără a fi afectată finanțarea altor activități deja planificate. Acestea au dorit ca activitatea de evaluare a organizației și de implementare a măsurilor de conformare la RGPD să nu deturneze concentrarea firmei (management, angajați) de la scopurile operaționale generatoare de profit.

Tipuri de oferte referitoare la activitățile de consultanță RGPD

Din punct de vedere al modalităților de realizare a consultanței, există 2 abordări majore:

- **Consultanța ON-LINE**, care se realizează pe baza unui audit preliminar (completarea unui chestionar de către beneficiar și emiterea unor recomandări de către prestatorul de servicii). Consultantul pune la dispoziție și modele pentru documentele care trebuie întocmite de către beneficiar, sub îndrumarea consultantului. Legătura între consultant și beneficiar se ține prin intermediul unei platforme on-line. *Acest tip se abordare este specific caselor de avocatură și firmelor specializate în IT*.

- **Consultanța bazată pe culegerea directă a informațiilor de către consultant** (prin completarea chestionarului de către acesta, în urma discuțiilor purtate cu factorii de decizie ai organizației și cu persoanele cu responsabilități pe linia prelucrării datelor cu caracter personal), verificarea ”în teren” a informațiilor și a modului în care sunt prelucrate datele cu caracter personal, studierea contractelor încheiate cu persoanele împuternicite sau operatorii asociați, analizarea soluțiilor informatice utilizate la nivelul operatorului. Legătura dintre consultant și beneficiar se realizează direct, iar documentele necesare sunt întocmite de către consultant. *Acest tip de abordare este specific firmelor de consultanță care au capabilități complexe de expertiză: analiză organizațională, securitate organizațională, IT, juridic.*

Tipuri de clienți pentru consultanța GDPR

Din punct de vedere al obiectivului vizat prin apelarea la consultanța GDPR, există următoarele tipuri principale de clienți:

Tipul 1: Clienți care vizează realizarea conformității organizației la cerințele RGPD, pe fondul unei culturi organizaționale condusă după principiul general al legalității activității desfășurate. Aceștia doresc ca, în urma activității de consultanță, organizația să îndeplinească, în mod real, toate cerințele organizatorice și tehnice prevăzute de RGPD.
Tipurile de organizații: *în general, firme mijlocii și mari eficiente economic, cu o cultură organizațională puternică*

Tipul 2: Clienți care inițial urmăresc să evite potențialele amenzi ale ANSPDCP, iar, ulterior, întrucât tot investesc bani în consultanță, iau decizia ca respectiva activitate să conducă la îndeplinirea, în mod real, a cerințelor RGPD.
Tipurile de organizații: *în general, firme mici, mijlocii și mari eficiente economic, aflate într-o dezvoltare rapidă, fără o cultură organizațională bine definită în această etapă*

Tipul 3: Clienți care urmăresc doar să evite potențialele amenzi ale ANSPDCP și doresc doar crearea unor probe de suprafață, ca dovezi ale conformității cu RGPD. Aceștia nu vizează în mod real implementarea, la nivelul organizației, a cerințelor RGPD.
Tipurile de organizații: *în general, firme mici, mijlocii și mari ineficiente economic, fără o cultură organizațională bine definită.*

Ce tipuri de consultanți preferă clienții? (1)

I. Majoritatea clienților de **tip 1** și de **tip 2** preferă legătura directă, personală cu consultantul, întrucât astfel au un anumit tip de control asupra modului de derulare a misiunii de consultanță.

De exemplu, conducerea firmei beneficiare se simte confortabil dacă, la finalul unei zile în care consultanții au studiat documentele firmei sau au discutat cu angajații, aceștia îi fac o scurtă informare verbală și, mai ales, îi prezintă situațiile care necesită o intervenție de urgență.

De asemenea, prin discuții, le pot fi indicate consultanților zonele organizației care necesită o atenție sporită din partea acestora.

Un alt aspect care este luat în calcul de beneficiarii de **tip 1** și **2**, este acela că simpla prezență în firmă a consultanților RGPD face ca salariații să conștientizeze că, la nivelul respectivei organizații, vor avea loc, cel mai probabil, schimbări majore pe linia activității de prelucrare a datelor cu caracter personal.

Ce tipuri de consultanți preferă clienții? (2)

II. Majoritatea clienților de **tip 3** apelează la consultanța on-line, care, invariabil, promite punerea la dispoziție a unor documente care pot fi prezentate ANSPDCP, clienților sau partenerilor de afaceri pentru demonstrarea conformității la RGPD.

În realitate, aceștia ajung să aibă doar la nivel declarativ măsuri tehnice și organizatorice adecvate și evită, prin orice mijloace, să facă proba măsurilor de asigurare a securității datelor cu caracter personal prelucrate ca operator asociat sau persoană împuternicită.

Această abordare „acceptabilă la prima vedere“ se va dovedi nefolositoare la primul contact cu ANSPDCP, cu un operator pentru care se acționează ca persoană împuternicită sau cu o persoană vizată care dorește să-și exercite drepturile conferite de RGPD.

Confidențialitatea în activitatea de consultanță RGPD

Întrucât, cu ocazia desfășurării activităților specifice, consultanții au acces direct sau indirect în profunzime la o multitudine de informații sensibile ale beneficiarului (ex. contracte comerciale, documente referitoare la organizarea și funcționarea firmei etc.), în contractul de consultanță este foarte importantă existența clauzelor referitoare la confidențialitatea informațiilor.

Consultantul este un prestator de servicii, deci va trebui să demonstreze, la rândul lui, că a dispus măsuri organizatorice și tehnice adecvate pentru protejarea informațiilor preluate de la Beneficiar.

Exemplu – firma STABRIS

- Culegerea informațiilor se face direct la sediul beneficiarului
- Documentele sunt studiate la sediul beneficiarului (nu se preiau copii după documentele studiate)
- Consemnarea informațiilor se face direct într-o zonă privată de stocare, „*cloud*“-ul firmei, laptopurile consultanților fiind conectate prin canal VPN la serverul criptat al firmei
- Comunicarea cu beneficiarul se face doar prin e-mail-uri criptate transmise între serverele de e-mail ale consultantului și firmei beneficiare.

CONCLUZII

- Activitatea de consultanță RGPD este încă la un stadiu incipient de dezvoltare.
- Trebuie luat în considerare faptul că rezultatele privind conformitatea la RGPD pot fi obținute într-un termen mai scurt cu sprijinul unei firme de consultanță, dar nu sunt realiste soluțiile „instant“ propuse/promise de unii ofertanți de consultanță.
- Rezultatul activităților de consultanță ar trebui să fie constituit dintr-un set de recomandări corecte din punct de vedere al realizării conformității cu RGPD, posibil de pus în aplicare la nivelul firmelor beneficiare, care să fie generate în baza unei evaluări exhaustive a problematicii prelucrării datelor cu caracter personal la nivelul organizației beneficiare.
- Confidențialitatea activităților de consultanță RGPD este foarte importantă și trebuie consemnată în mod explicit în contractul încheiat între prestatorul de servicii și organizația beneficiară.

Vă mulțumesc!

Cristian OBREJA

Manager STABRIS

office@stabris.ro