”GDPR – de la intrebari la raspunsuri”

De ce **”de la intrebari, la raspunsuri”**? Pentru ca in mod cert, la finalul lecturarii Regulamentului 679/ 2016, dincolo de intelegerea precisa a obiectivelor urmarite si a principiilor legate de prelucrarea datelor cu caracter personal - ce sunt foarte clar enuntate de Regulament - orice cititor mai mult sau mai putin avizat, ramane invariabil in minte cu o multitudine de intrebari despre **”cum”** si **”in ce mod”** obiectivele pot fi atinse, iar principiile pot fi respectate in practica.

Atunci cand vine vorba despre companii, operatori de date cu caracter personal, e nu doar firesc ci chiar necesar ca acestia sa analizeze in mod critic cerintele regulamentului, sa identifice intrebarile corecte si sa caute raspunsurile potrivite.

Dupa cum stim, companiile dispun de o perioada intermediara pana la care – in lumina principiului responsabilitatii definit de Regulament – sa stabileasca ce au de facut si sa puna in practica masurile necesare – de natura tehnica si organizatorica – pentru a se conforma incepand cu 25 mai 2018 regulilor GDPR.

Cum masurile tehnice sunt apanajul altor experti, in cadrul acestui colocviu juridic imi propun sa tratez unele dintre masurile organizatorice la care fiecare operator ar trebui sa se gandeasca. Asadar, a propos de intrebarile corecte la care – spuneam mai sus – fiecare operator ar trebui sa gaseasca un raspuns, cred ca orice operator de date cu caracter personal si in special aceia care au un numar mare de angajati, ar trebui sa-si puna urmatoarele intrebari:

Oare toti angajatii din cadrul companiei stiu exact ce inseamna noile reguli de confidentialitate si care este impactul lor asupra proceselor interne? Cum ne asiguram ca toti angajatii companiei inteleg si actioneaza in sensul respectarii cerintelor GDPR?

Raspunsul la aceste intrebari este, desigur, unul complex. Si presupune ca fiecare operator sa planifice un proces de implementare a GDPR **(i)** in cadrul caruia sa identifice actiunile necesare, momentul la care acestea trebuie intreprinse si sa aloce un buget corespunzator si **(ii)** la finalul caruia toti angajatii sai sa poata sa raspunda, la randul lor, la o serie de intrebari pe care le voi enunta in continuare.

Pentru a exemplifica in concret anumite situatii practice legate de prelucrarea datelor, ma voi raporta, in cateva ocazii, la modul de prelucrare a datelor apartinand chiar angajatilor. Astfel,

1. O prima intrebare ar fi: *”De ce trebuie sa respectam regulile in materie de protectie a datelor cu caracter personal?”*

Angajatii operatorilor implicati in procesele ce presupun prelucrarea de date trebuie sa fie constienti de importanta respectarii regulilor de data protection, de fiecare data cand

colecteaza, inregistreaza, organizeaza, structureaza, stocheaza, adapteaza sau modifica, extrag, consulta, utilizeaza, divulga, combina, restrictioneaza, sterg sau distrug astfel de date. Enumerarea este lunga, dar toate aceste operatiuni se circumscriu notiunii generice de ”prelucrare a datelor”.

Aceasta importanta despre care vorbim este data:

- **pe de o parte, de interesul ocrotit de Regulament**: unul general de asigurare a protectiei drepturilor si libertatilor fundamentale ale persoanelor fizice in ceea ce priveste prelucrarea datelor lor cu caracter personal,
- **pe de alta parte, de regimul sanctionator sever** aplicabil in cazul neconformarii cu cerintele Regulamentului. Limita maxima a amenzii ajunge pana la 20 de milioane EUR sau 4% din cifra de afaceri mondiala totala anuala, pentru incalcarea acelor obligatii referitoare la:
    - principiile de baza ale prelucrarii (inclusiv conditiile privind existent, atunci cand este cazul, a consimtamantului - care trebuie sa fie specific si lipsit de echivoc);
    - drepturile persoanelor vizate;
    - transferurile de date cu caracter personal catre un destinatar dintr-o tara tetra.

2. O data lamurita importanta subiectului, angajatii ar trebui sa-si puna intrebarea: *”Sunt autorizat pentru accesarea si prelucrarea categoriilor de date cu care operez?”*

Raspunsul ar trebui sa se regaseasca, in primul rand, in cuprinsul procedurilor interne sau al altor materiale scrise, disponibile angajatilor, pentru a caror completare/elaborare este necesar ca fiecare operator sa faca o analiza temeinica in scopul reidentificarii structurilor si angajatilor ale caror atributii implica procesarea de date cu caracter personal, pe diverse categorii de persoane vizate (ex. clienti, furnizori, salariati etc).

De exemplu, persoanele care prelucreaza datele cu caracter personal ale angajatilor operatorului sunt cei implicati in procesele de:

- ✓ recrutare si angajare
- ✓ monitorizare a modului de executare a atributiilor, conform contractului de munca, inclusiv monitorizarea registrului de evidenta a activitatii, a registrului de intrari-iesiri, a rapoartelor de activitate generate de diverse aplicatii IT, a emailurilor transmise;
- ✓ delegare a drepturilor de semnatura;
- ✓ calcul si plata a salariilor si a altor drepturi;

- ✓ asigurare a sanatatii si securitatii la locul de munca;
- ✓ monitorizare a conflictelor de interese, cum este cazul institutiilor de credit ce au obligatii specifice in acest sens, derivand din legislatia speciala;
- ✓ monitorizare a respectarii obligatiilor de confidentialitate privind informatiile companiei si clientilor/partenerilor acesteia;
- ✓ acordare a accesului la aplicatiile informatice ale companiei si asigurarii securitatii acestora;
- ✓ aplicare de sanctiuni disciplinare;
- ✓ incetare a raporturilor de munca;
- ✓ realizare a apararilor in cadrul eventualelor litigii cu salariatii, etc

Ulterior reanalizarii activitatii structurilor organizatorice si suplimentar reglementarii in proceduri a **(i)** categoriilor de date cu caracter personal pe care salariatii acestora le pot prelucra si a **(ii)** modalitatii in care prelucrarea se realizeaza, ar trebui ca, pentru fiecare categorie de angajati, sa fie stabilite si organizate:

- ✓ programe adaptate de training in materie de prelucrare adecvata a datelor;
- ✓ acordarea de drepturi diferentiate de acces la date cu caracter personal (de exemplu, doar o categorie restransa de persoane va avea acces la informatiile privind veniturile salariatilor);
- ✓ evidente ale persoanelor care au prelucrat anumite date cu caracter personal;
- ✓ metodele de asigurare a securitatii datelor cu caracter personal;
- ✓ controale tehnice si testari periodice pentru a asigura conformitatea.

Toate acestea se vor constitui pentru angajati in surse suplimentare de clarificare a rolului lor si a masurii in care sunt autorizati sa aiba acces si sa prelucreze categoriile de date cu care opereaza.

3. In cazul operatorilor cu activitate complexa, ce presupune implicarea unor alte persoane, din afara companiei, in procesul de prelucrare a datelor, angajatii ar trebui sa se intrebe: *”In ce conditii pot avea alte persoane acces la datele cu caracter personal colectate de noi?”*

In cazul in care unele dintre activitatile operatorului sunt delegate ori realizate prin intermediul unor persoane imputernicite (cum sunt, in cazul institutiilor de credit, furnizorii unor servicii externalizate), companiile au obligatia de a incheia cu acestia un contract scris, de a tine o lista actualizata a acestor persoane imputernicite, precum si, in plus, de a face o evaluare a persoanelor imputernicite in ceea ce priveste garantiile oferite de acestea din perspectiva GDPR, in special in ceea ce priveste cunostintele de specialitate, fiabilitatea proceselor si sistemelor, resursele.

In ceea ce priveste contractele in curs de derulare cu astfel de furnizori/ persoane imputernicite, este necesar ca, in vederea asigurarii respectarii, incepand cu data de 25 mai 2018, a principiilor si cerintelor stabilite de GDPR, operatorii sa parcurga un proces de revizuire a acestor angajamente contractuale. O atare revizuire ar trebui sa vizeze cel putin clauzele privitoare la:

- ✓ obiectul si durata prelucrarii datelor
- ✓ natura si scopul prelucrarii
- ✓ tipul de date cu caracter personal si categoriile de persoane vizate
- ✓ obligatiile si drepturile operatorului
- ✓ obligatiile ce revin persoanelor imputernicite si angajatilor acestora in vederea respectarii prevederilor GDPR, inclusiv confidentialitatea si masurile in materie de securitate tehnica si organizatorica).

4. Un alt aspect pe care angajatii ar trebui sa-l cantareasca, ar fi: *"Este intr-adevar necesara prelucrarea datelor pentru desfasurarea activitatii mele?"*

Va trebui ca angajatii identificati ca fiind autorizati pentru accesarea si prelucrarea anumitor categorii de date sa ajute la intocmirea unui inventar general al datelor personale prelucrate in legatura cu realizarea activitatii lor.

Spre exemplu, in cazul prelucrarii datelor celorlalti angajati ai companiei, nu doar datele cu caracter personal vadit, precum nume, CNP, adresa etc. sunt relevante, ci si orice alte date care permit identificarea salariatului, cum ar fi, in anumite situatii:

- ✓ numarul de marca unic atribuit unui salariat
- ✓ credentialele pentru autentificare pe statia de lucru sau in diverse aplicatii informatice
- ✓ numarul de telefon
- ✓ emailul
- ✓ ID-urile cookie-urilor
- ✓ identificatorii online, identificatorii dispozitivelor si adresele IP (relevante, de exemplu, in cazul dispozitivelor mobile).
- ✓ datele din registrul de evidenta a activitatii sau din registrul de intrari/iesiri

In realizarea acestui inventar al datelor, angajatii care prelucreaza datele trebuie sa analizeze in mod critic ce tipuri de date pot permite identificarea unei persoane si sa se gandeasca la toate

mijloacele pe care este probabil, in mod rezonabil, sa le utilizeze compania sau orice alta persoana in scopul identificarii unei persoane fizice determinate.

In ceea ce priveste tipurile de noi prelucrari pe care operatorul ar urma sa le efectueze ulterior intrarii in vigoare a Regulamentului, GDPR prevede obligatia acestuia ca, inaintea efectuarii respectivelor prelucrari, sa realizeze o evaluare a impactului operatiunilor de prelucrare asupra protectiei datelor cu caracter personal. Angajatii operatorului trebuie sa cunoasca aceasta obligatie si sa solicite la timp consilierea Responsabilului cu Protectia Datelor, asa incat procesul cerut de Regulament sa fie respectat intocmai.

Lista ce va detalia tipurile de operatiuni care vor face obiectul cerintei de efectuare a unei asemenea evaluari urmeaza a fi intocmita si publicata de catre ANSPDCP. Daca rezultatele evaluarii interne efectuate de operator ar indica faptul ca prelucrarea ar genera un risc ridicat in absenta unor masuri luate de operator pentru atenuarea acestuia, operatorul are, de asemenea, obligatia de a consulta ANSPDCP, in calitate de autoritate de supraveghere.

5. Angajatii ar trebui, in plus, sa se intrebe: *”Este necesara colectarea tuturor datelor? S-ar putea atinge scopul pentru care sunt colectate datele, prin folosirea unui volum mai mic de date cu caracter personal ori a unor date mai putin sensibile? ”*

Uneori, din cauza unui grad prea mare de standardizare in procesul de colectare a datelor, s-ar putea sa fie colectate date care sunt nenecesare, iar acest lucru contravine principiului reducerii la minimum a datelor, potrivit caruia datele cu caracter personal prelucrate trebuie sa fie adecvate, relevante si limitate exclusiv la ceea ce e necesar.

De exemplu, printr-un formular-standard, angajatilor li se poate solicita in prezent, la angajare, sa furnizeze date cu privire la detinerea unui permis de conducere. Insa doar o parte dintre angajati vor fi autorizati sau indreptatiti sa foloseasca o masina a companiei. Prin urmare, colectarea acestei informatii ar trebui realizata doar de la salariatii carora compania ar urma sa le puna la dispozitie sau sa le solicite sa conduca o masina.

Asadar, pentru a stabili in ce masura este necesara colectarea tuturor datelor pe care in prezent compania obisnuieste sa le solicite, se impune revizuirea critica de catre angajatii relevanti si sub indrumarea responsabilului cu protectia datelor, a tuturor documentelor prin intermediul carora datele cu caracter personal sunt obtinute (ex. chestionare, contracte, formulare) si analizarea faptului daca, pentru fiecare tip de data, operatorul are o obligatie legala sau un interes legitim sa prelucreze respectiva informatie.

6. Ar trebui de asemenea ca angajatii sa se preocupe si sa stie raspunsul la intrebarea: *”Ce ar trebui facut cu datele care au fost colectate in plus?”*

Desi este discutabil in ce masura GDPR se aplica datelor colectate anterior intrarii sale in vigoare, este recomandabil ca acestea sa fie identificate si sterse, in masura in care aceasta optiune nu se dovedeste a fi imposibila sau nu ar implica eforturi disproportionate.

7. O alta intrebare utila din perspectiva conformarii la cerintele GDPR este: *"Pot sa prelucrez date cu caracter personal privind condamnarile penale? In ce conditii se poate cere cazier judiciar?"*

Raspunsul la aceasta intrebare comporta o analiza detaliata a dreptului intern si a garantiilor adecvate pentru drepturile si libertatile persoanelor vizate, ce poate si trebuie sa fie facuta cu implicarea Responsabilului cu Protectia Datelor.

Luand insa exemplul unei institutii de credit, care prelucreaza si ar urma sa prelucreze si dupa data de 25 mai 2018 astfel de date, in legatura cu salariatii sau candidatii pentru anumite posturi, aceasta trebuie sa se asigure ca o astfel de prelucrare este permisa sau impusa fie de legislatia muncii fie de legislatia bancara specifica (ex. in privinta conducatorilor sau a persoanelor angajate ca gestionari). Totodata, orice astfel de prelucrare trebuie sa fie insotita de garantii adecvate pentru drepturile si libertatile persoanelor vizate.

8. Angajatii care lucreaza in departamentele de Securitate sau altele cu atributii similare, in mod rezonabil ar putea sa se intrebe: *"Pot sa monitorizez corespondenta si comunicatiile electronice ale angajatilor?"*

Luand cazul institutiilor de credit, monitorizarea corespondentei si a comunicatiilor electronice ale angajatilor nu este doar un drept, ci si o obligatie legala, derivand din cerintele specifice in materie de prudenta si secret profesional.

Datele clientilor si ale angajatilor proprii, precum si increderea acestora reprezinta, poate, cel mai de pret activ al unei institutii de credit. Prin urmare, asemenea monitorizari sunt permise, desigur insa cu respectarea celorlalte cerinte si garantii in materia protectiei datelor, astfel incat sa fie respectate drepturile si libertatile angajatilor, foarte important fiind modul in care aceasta monitorizare este realizata, respectiv daca:

- ✓ mijloacele de comunicatie sunt puse la dispozitie de angajator?
- ✓ angajatorul i-a facut cunoscut angajatului ce ii este permis si ce ii este interzis?
- ✓ angajatul a fost informat si este constient de monitorizare si de scopul acesteia? Cum s-a realizat aceasta informare?
- ✓ angajatorul a respectat scopul monitorizarii declarat angajatului?

O atare intelegere este confirmata si de practica recenta a Curtii Europene a Drepturilor Omului care s-a pronuntat in sensul ca angajatorul poate monitoriza corespondenta si comunicatiile electronice ale angajatului atunci cand exista un just echilibru intre interesele angajatorului si dreptul la viata privata al angajatului si numai daca angajatorul ii face cunoscut angajatului ce este sau nu permis si il informeaza asupra oricaror forme de monitorizare care vor fi implementate.

9. Angajatii care lucreaza in relatie directa cu persoanele vizate/ clientii, ar putea sa se intrebe: *"In ce mod trebuie sa furnizez persoanelor vizate informatiile necesare privitoare la procesarea datelor lor?"*

In conformitate cu principiul transparentei, orice informatie adresata persoanei vizate dar si publicului trebuie sa fie furnizata intr-o forma concisa, transparenta, inteligibila si usor accesibila, folosind un limbaj clar si simplu. Informatiile trebuie furnizate in scris si / sau prin mijloace electronice. La solicitarea persoanei vizate, informatiile pot fi furnizate oral, cu conditia insa ca identitatea persoanei vizate sa fie dovedita prin alte mijloace.

Pentru a oferi o imagine de ansamblu usor vizibila si semnificativa asupra procesarii de date ce se intentioneaza a fi desfasurata, informatiile pot fi furnizate in combinatie cu pictograme standardizate.

10. Ar trebui, de asemenea, sa se intrebe angajatii: *"Exista un cod de conduita pe care trebuie sa il respect?"*

Fiecare angajat va trebui sa cunoasca existenta si prevederile Codului de Conduita la care a aderat sau va adera compania pentru care lucreaza.

In economia GDPR, este incurajata elaborarea de Coduri de Conduita de catre asociatii si alte organisme care reprezinta categorii de operatori sau de persoane imputernicite, menite sa contribuie la o buna aplicare a Regulamentului, tinand seama de caracteristicile specifice ale diverselor sectoare de activitate. Aceste Coduri, o data avizate din punct de vedere al conformitatii cu Regulamentul si aprobate de catre autoritatea de supraveghere competenta, in cazul in care se constata ca ofera garantii adecvate si suficiente, sunt relevante dintr-o tripla perspectiva:

- **in primul rand**, aceea ca orice companie care adera la respectivul cod, isi asuma un angajament ferm de respectare a acestuia fiind prezumata a oferi ea insasi garantii suficiente si un nivel adecvat de protectie a datelor,
- **in al doilea rand** din perspectiva reputatiei si al increderii publice, extrem de importante indiferent de domeniul in care activeaza operatorul,

- **in al treilea si nu in ultimul rand**, din perspectiva faptului ca acest aspect va fi avut in vedere drept un factor atenuant de catre autoritatea de supraveghere cu ocazia unor eventuale investigatii.

11. O alta intrebare importanta care ar trebui sa preocupe angajatii este: *"Cat timp pot sa pastrez datele cu caracter personal?"*

Angajatii trebuie sa cunoasca faptul ca obligatia de a asigura protectia si confidentialitatea datelor cu caracter personal incepe o data cu procesul de colectare a datelor si inceteaza la data stergerii acestora, dar, in egala masura, ca obligatia de confidentialitate continua si dupa aceasta data in ce priveste informatiile de care angajatii au luat cunostinta in cursul exercitarii atributiilor lor.

Datele cu caracter personal nu trebuie sa fie pastrate mai mult decat este necesar pentru realizarea scopului in care au fost colectate, cu exceptia cazului in care exista o obligatie legala sau un interes legitim al operatorului. In masura in care se apreciaza ca datele ar putea fi utilizate, ulterior, si in alte scopuri, se poate cere acordul persoanei vizate pentru prelucrarea acestora in noul scop adus la cunostinta acesteia. Spre exemplu, CV-urile candidatilor pot fi pastrate si dupa ce postul pentru care au candidat a fost ocupat, in scopul unei reanalizari viitoare a candidatului in legatura cu alte pozitii ce ar deveni eventual disponibile, insa cu conditia ca respectivul candidat sa fie informat in mod corespunzator pentru a-i da acestuia posibilitatea sa se opuna si/sau sa solicite stergerea informatilor.

In ceea ce priveste durata de arhivare a documentelor, aceasta se stabileste prin nomenclatoare arhivistice, aprobate de organele de conducere ale operatorului, precum si de Arhivele Nationale.

In contextul GDPR, toti operatorii vor trebui sa se asigure ca revizuiesc aceste nomenclatoare si ca acestea sunt aduse la cunostinta angajatilor relevanti.

****

Intrebarile de mai sus sunt doar cateva din multitudinea celor care necesita un raspuns. Data de 25 mai 2018 va marca un moment cheie si un nou inceput in ceea ce priveste prelucrarea datelor cu caracter personal.

Compexitatea subiectului si implicatiile multiple pe care le are modul in care gestionam datele cu caracter personal vor presupune o continua interpretare a prevederilor Regulamentului si un proces constant de invatare si de adaptare. In acest sens, asteptam cu interes emiterea de catre Comitetul European pentru protectia datelor de orientari, recomandari si bune practice in aplicarea coerenta a Regulamentului. In egala masura, este de subliniat rolul si importanta ANSPDCP, in calitate de autoritate nationala de supraveghere, inclusiv in ceea ce priveste faptul ca, prin reglementarile si opiniile pe care le va emite, va contura raspunsurile pentru lamurirea aspectelor inca incerte, insuficient detaliate de Regulament sau in privinta carora Regulamentul permite optiuni nationale.

Diana Ciubotariu 23.10.2017
Director Directia Juridica
UniCredit Bank S.A.