GDPR

Cum începem?

Ghid de bune practici privind prelucrarea datelor cu caracter personal în cadrul activității profesiei de contabil și auditor financiar

Important

Informațiile și îndrumările din cuprinsul acestui document sunt menite să contribuie la o mai bună înțelegere a normelor UE privind protecția datelor. Instrumentul acesta are un rol pur orientativ. Doar textul GDPR poate crea drepturi și obligații pentru persoanele fizice sau persoanele juridice.

Explicațiile oferite în acest Ghid au doar un scop informativ. Datorită naturii complexe a legislației, precum și datorită aspectelor personale ale situației expuse de dumneavoastră, este posibil ca sfaturile oferite prin intermediul Ghidului să nu fie aplicabile în situația particulară în care vă aflaţi. Înainte de a lua decizia utilizării acestui Ghid la situația dvs. particulară, vă rugăm să consultați un specialist în aplicarea GDPR.

Nici CAFR sau avocatnet.ro și nici vreo persoană care acționează în numele CAFR ori avocatnet.ro nu este responsabilă pentru posibila utilizare a informațiilor următoare.

Cuprins

Introducere

În 25 mai va intra în vigoare Regulamentul European privind Protecția Datelor Personale (GDPR în forma pe care o cunoaște deja toată lumea). Știm că e foarte important să aveți acces la resurse credibile și adaptate nevoilor dumneavoastră, în privința GDPR.

Regulamentul vizează foarte multe aspecte ale activității unui contabil sau auditor financiar, motiv pentru care am constituit o echipă multidisciplinară, menită să lucreze la elaborarea unui Ghid de bune practici privind impactul GDPR în activitatea profesiei de contabil sau auditor financiar.

Ghidul de mai jos este rezultatul acestei colaborări. Vom reveni, în lunile următoare, cu ediții actualizate ale Ghidului, pe măsură ce vor apărea elemente practice de natură să explice mai bine unele prevederi ale GDPR.

De ce un Regulament și nu o Directivă?

GDPR vine de la ***General Data Protection Regulation***, pe numele său tradus *Regulamentul 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE* (Regulamentul general privind protecția datelor – n.a.).

Regulamentele sunt acte normative ale Uniunii Europene care au **forță juridică obligatorie în fiecare stat membru** și intră în vigoare la o dată stabilită, în același timp, în toate statele membre.

Spre deosebire de Regulamente, Directivele stabilesc o direcție, stabilesc anumite rezultate care trebuie realizate, dar fiecare stat membru trebuie să transpună textul Directivei în legislația națională. Cu alte cuvinte, pentru ca o Directivă să intre în vigoare, e nevoie ca ea să fie transpusă într-o lege națională, care lege să fie apoi adoptată de Parlamentul țării în cauză.

De aceea, Directivele au nevoie de tot atâtea legi naționale de transpunere câte state fac parte din Uniunea Europeană, pentru a putea să-și producă efectele. Din cauza acestei situații, aplicarea unei Directive poate să fie extrem de complicată, la nivel unitar, în toate statele Uniunii Europene. Diferențele de interpretare sau aplicare sunt, uneori, notabile.

Ca să înlăture această situație, Regulamentul, ca tip de act normativ european, vine cu o abordare nouă. El **se aplică unitar, deodată, în toate statele UE**. Statele au, de asemenea, mici marje de manevră în privința adoptării unor legi naționale care să adapteze unele prevederi ale Regulamentului (menționate explicit de acesta) la cultura sau specificul național. Pentru a activa aceste marje de manevră, statele pot emite ceea ce poartă numele de Legi privind aplicarea GDPR în legislația națională. Însă intrarea în vigoare se întâmplă deodată, pentru toate statele UE, indiferent de ce spun aceste legi naționale. Intrarea în vigoare și, deci, aplicarea Regulamentelor nu depinde de adoptarea acestor legi naționale și nici nu e condiționată de aceasta.

Mai mult, Parlamentele naționale, Guvernele sau orice alte organisme interne care au atribuții specifice în domeniul legislativ sau executiv nu pot înlătura sau împiedica intrarea în vigoare a Regulamentelor europene în statele în cauză.

Specificațiile de mai sus au menirea de a sublinia că **intrarea în vigoare a GDPR nu poate fi amânată sau suspendată** nici de Parlamentul României, nici de Guvern printr-o Ordonanță de Urgență (atât de întâlnită în ultimii zeci de ani la noi). **25 mai** este termenul de intrare în vigoare în toate statele Uniunii Europene și **acest termen nu se va schimba**.

Și mai important: **Regulamentul a intrat în vigoare în mai 2016** și a stabilit că, **până la 25 mai 2018**, statele membre și organizațiile cărora li se va aplica acesta vor avea timp de adaptare și acomodare cu prevederile Regulamentului. Prin urmare, a existat deja o perioadă de grație de 2 ani, în care atât statele membre (care trebuiau să promoveze existența Regulamentului și să educe piața), cât și organizațiile (cărora li se va aplica Regulamentul) să se obișnuiască cu prevederile acestuia.

Din acest capitol, trebuie reținute deci două lucruri:

1. Vorbim despre un Regulament european, nu despre o Directivă.
2. Acest Regulament a intrat în vigoare in mai 2016 și se va aplica, unitar, în toate statele Uniunii Europene, de la data de 25 mai 2018, indiferent de ce acțiuni vor întreprinde autoritățile naționale.

De ce tot facem referire la „Grupul de Lucru Articol 29”?

„Grupul de Lucru Articol 29” este un organism consultativ creat din reprezentanți ai Autorităților de Supraveghere ai statelor membre UE, alături de care mai sunt reprezentate Autoritatea Europeană de Supraveghere a Protecției Datelor, precum și Comisia Europeană.

Se numește astfel pentru că structura și scopul său au fost create prin aplicarea Articolului 29 al Directivei privind Protecția Datelor Personale. Grupul de Lucru a fost lansat în 1996.

Grupul de Lucru a fost creat pentru a:

- Oferi consultanță Statelor UE cu privire la implementarea legislației privind protecția datelor personale;
- Promova aplicarea unitară a Directivei privind Protecția Datelor Personale în UE și Zona Economică Europeană;
- Oferi Comisiei o opinie asupra legislației comunitare primare care afectează dreptul la protecția datelor cu caracter personal;
- Oferi recomandări pentru public, în materii legate de protecția datelor cu caracter personal.

Odată cu apariția Regulamentului General privind Protecția Datelor cu Caracter Personal (GDPR), care înlocuiește Directiva privind Protecția Datelor cu Caracter Personal, se va schimba și Grupul de Lucru într-un organism cu un rol mult mai important.

Astfel, de la 25 mai, Grupul de Lucru va deveni Comitetul European pentru Protecția Datelor (CEPD). Acesta are în componență șefii fiecărei Autorități de Supraveghere Naționale (APD), precum și șeful Autorității Europene pentru Protecția Datelor (AEPD) sau reprezentanții acestora. Comisia Europeană participă la reuniunile CEPD fără a avea drept de vot. Secretariatul CEPD este asigurat de AEPD.

CEPD va fi în centrul noului sistem de protecție a datelor în UE. Acesta va contribui la asigurarea aplicării consecvente a legii privind protecția datelor în întreaga UE și va depune eforturi pentru a asigura cooperarea eficace între APD-uri. Comitetul nu numai că va publica orientări privind interpretarea conceptelor principale ale RGPD, dar va fi solicitat și să ia decizii obligatorii în cazul unor litigii privind prelucrarea transfrontalieră, asigurând astfel o aplicare uniformă a normelor UE pentru a evita tratarea diferită a aceluiași caz în diferite jurisdicții.

Concepte importante pentru înțelegerea GDPR

Prelucrare de date

Prin prelucrarea datelor se înțelege orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi:

- colectarea;
- înregistrarea;
- organizarea;
- structurarea;
- stocarea;

- adaptarea sau modificarea;
- extragerea;
- consultarea;
- utilizarea;
- divulgarea prin transmitere;
- diseminarea sau punerea la dispoziție în orice alt mod;
- alinierea sau combinarea;
- restricționarea;
- ștergerea sau distrugerea.

După cum se observă, prezența sintagmei "cum ar fi" în corpul acestei definiții face enumerarea să fie una exemplificativă, nu una limitativă. Cu alte cuvinte, se pot imagina și alte activități care intră în sfera ideii de prelucrare, în afara celor enumerate mai sus.

Dacă ar fi să reducem această definiție la un limbaj comun, ar trebui să spunem că, **prin prelucrarea datelor cu caracter personal se înțelege orice gen de activitate care este realizată cu și asupra acelor date, de la momentul colectării lor (inclusiv) și până la momentul distrugerii lor (inclusiv).**

Date cu caracter personal

Unde se regăsește informația în GDPR?

Articolul 2, articolul 4 punctele 1 și 5 și considerentele (14), (15), (26), (27), (29) și (30) ale GDPR.

Definiția datelor cu caracter personal

Potrivit GDPR, „date cu caracter personal" înseamnă **orice informații privind o persoană fizică identificată sau identificabilă** („persoană vizată"). O persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

Nu există o listă a datelor cu caracter personal, iar GDPR nu impune statelor să realizeze o astfel de listă, pentru simplul motiv că o dată poate deveni într-un anumit context **dată cu caracter personal**, iar în alt context să fie pur și simplu o informație fără valoare de dată cu caracter personal.

Enumerarea din definiția de mai sus e una **exemplificativă** și nu are caracterul de a "limita" în mod absolut datele cu caracter personal doar la cele enumerate acolo.

Exemple de date cu caracter personal:

- numele;
- domiciliul sau reședința cuiva;

- o adresă de e-mail (inclusiv adresele de tipul prenume.nume@firma.ro);
- numărul de buletin, pașaport sau carte de identitate;
- date privind locația (de exemplu, funcția de date privind locația disponibilă pe un telefon mobil)*;
- un IP;
- un cookie ID;
- silueta cuiva din înregistrările CCTV;
- un număr de înmatriculare al unei mașini;

În același timp, însă, pentru a exemplifica momentul în care o informație poate fi sau nu o dată cu caracter personal, dacă presupunem că o persoană găsește pe jos o hârtie pe care e scris numărul 4.930, fără nicio altă informație ajutătoare, atunci acea informație e imposibil de legat de o anumită persoană. Nu vorbim, deci, despre o informație care ar putea fi dată cu caracter personal.

Dacă, însă, cineva găsește pe jos o hârtie pe care este scrisă suma de 4.930 lei, cu mențiunea că e un salariu din firma SC X SRL, atunci acel cineva, dacă ar face o investigație și ar reuși să pună cap-la-cap informații (inclusiv prin discuția cu departamentul HR al companiei în cauză, o reclamație la ITM sau altele asemenea), ar putea afla (direct sau prin intermediul autorităților publice) că acel salariu aparține unei anumite persoane din companie. În acel context, informația respectivă devine data personală (pentru că se referă la o persoană identificabilă).

După cum se vede, definiția datelor cu caracter personal mai conține câteva elemente importante:

1) **Datele personale vizează informații privind persoanele fizice, nu persoane juridice.** Distincția e importantă pentru că, spre exemplu, numărul de înregistrare de la Registrul Comerțului, Codul fiscal ori alte elemente de identificare ale unor companii **nu sunt date cu caracter personal**. Mai mult, atunci când o adresă de e-mail ori un număr de telefon vizează în mod clar o persoană juridică (ex. e-mailurile de tip *office@* sau telefoanele de la un call-center public al unei companii), atunci nu vorbim despre date cu caracter personal.

2) **Nu contează dacă prelucrarea acestor date personale se face prin intermediul unui sistem automat ori prin intermediul unui sistem neautomatizat** (ex. manuale), dacă aceasta face parte dintr-un sistem structurat de evidență a datelor. Singurul lucru important e că vorbim despre o prelucrare a unui astfel de tip de date.

Mai multe informații pentru înțelegerea a ce sunt datele cu caracter personal se pot obține citind *Opinia nr. 4 din 2007 privind conceptul de date cu caracter personal*[1], emisă de Grupul de Lucru Articol 29. Simplificând definiția de mai sus, am putea concluziona că datele personale sunt acele **date care se referă la o persoană în viață care poate fi identificată**:

(a) direct, folosind aceste date; sau

(b) indirect, pornind de la aceste date și folosind informații suplimentare pe care este rezonabil să credem ca operatorul le-ar putea obține el însuși ori prin intermediul unor autorități implicate.

[1] http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_ro.pdf

Categorii speciale de date cu caracter personal

Un anumit tip de date personale, în cazul prelucrării cărora pot există consecințe importante pentru persoanele vizate, sunt numite de GDPR **"categorii speciale de date cu caracter personal"**.

Categoriile speciale date cu caracter personal sunt acelea care dezvăluie (conform art. 9 GDPR):

- originea rasială sau etnică;
- opiniile politice;
- confesiunea religioasă sau convingerile filozofice;
- apartenența la sindicate;
- date genetice;
- date biometrice pentru identificarea unică a unei persoane fizice;
- date privind sănătatea;
- privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

Prin „date genetice" înțelegem datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză.

Prin „date biometrice" înțelegem o dată cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice.

Prin „date privind sănătatea" înțelegem date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia.

Spre deosebire de datele personale "obișnuite", în cazul cărora GDPR folosește o enumerare exemplificativă, în cazul datelor personale cu caracter special, GDPR folosește o enumerare limitativă. Cu alte cuvinte, atunci când vorbim despre date cu caracter special, ne vom mărgini la această lista pentru identificarea datelor în cauză.

Acest tip de date e foarte important, pentru că prelucrarea sa nu e posibilă decât în condiții extrem de specifice, tratate în capitolele următoare.

Prelucrează un contabil ori un auditor financiar date speciale?

Dacă ne uităm peste lista care cuprinde enumerarea datelor speciale, o să observăm că un contabil sau un auditor prelucrează în multe situații astfel de date. Datele privind sănătatea sunt cel mai des întâlnite, dacă e să ne gândim doar la concediile medicale (date privind sănătatea) sau cererile de acordare a zilelor libere speciale ale salariaților de alte religii (date privind confesiunea religioasă), cu care unii contabili ori auditori se întâlnesc în anumite momente.

De asemenea, mai e de menționat că, în unele cazuri (vorbim totuși despre cazuri excepționale, care trebuie justificate ca atare), realizarea pontajului implică prelucrarea de date biometrice ale angajaților sau colaboratorilor (amprente, iris ori recunoaștere facială). Se întâlnesc situații în care prelucrarea acestor date, chiar dacă n-ar trebui să se întâmple așa, trece în "subordinea" departamentului de contabilitate.

Prin urmare, un contabil ori un auditor financiar prelucrează uneori și date cu caracter special și în aceste cazuri trebuie să se respecte condițiile speciale specificate într-unul dintre capitolele următoare ale acestui Ghid.

"Datele cu caracter personal" nu sunt echivalente cu "informațiile cu caracter personal"

De foarte multe ori, în contracte ori alte documente, se vorbește despre informații identificabile personal sau informații personale, laolaltă cu referirea la date personale. E important de definit foarte bine în actul respectiv ce se înțelege prin acele "informații personale" și dacă ele sunt sau nu sinonime pentru "datele cu caracter personal". Pentru că, altfel, ne putem trezi în situația exemplificată mai jos, când diferite legi ale unor state prevăd definiții speciale pentru "informațiile personale".

GDPR, definiție "date cu caracter personal"	**Definiție "informații cu caracter personal" din statutul privind notificarea incidentelor de securitate din Maryland, SUA**
Orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată");	"Primul nume al unui individ sau primul și ultimul nume în combinație cu unul sau mai multe următoarele elemente de date, atunci când numele sau elementele de date nu sunt criptate, redactate sau protejate în alt mod printr-o altă metodă care face ca informațiile să nu poată fi citite sau inutilizabile: (i) un număr de securitate socială; (ii) numărul permisului de conducere; (iii) un număr de cont financiar; (iv) un număr de identificare al unui contribuabil individual".

După cum se observă, între cele două concepte există o diferență majoră.

Operator

Potrivit GDPR, prin „operator" se înțelege o persoană fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește:

- scopurile și
- mijloacele de prelucrare a datelor cu caracter personal.

Opinia 1 din 2010 a Grupului de Lucru Articol 29, cu privire la conceptele de operator și împuternicit[2], definește foarte bine cele două concepte.

Rolul primordial al conceptului de operator este de a determina:

- cine este responsabil pentru respectarea normelor privind protecția datelor și
- modul în care persoanele vizate pot exercita drepturile în practică.

Cu alte cuvinte: rolul principal al operatorului este **să aloce responsabilitatea**. Simplist vorbind, Operatorul este "**creierul" operațiunilor de prelucrare** si el va răspunde întotdeauna pentru prelucrarea respectivă.

Împuternicit

„Persoană împuternicită de operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism **care prelucrează datele cu caracter personal în numele operatorului**.

Există două condiții esențiale pentru ca o entitate să se califice drept împuternicit:

- Să fie entitate juridică separată față de operator; și
- Să prelucreze date în numele operatorului; această activitate de prelucrare poate fi limitată la o activitate foarte specifică sau poate fi mai generală și mai extinsă.

Simplist vorbind, în multe cazuri, Împuternicitul este **instrumentul prin care Operatorul își realizează scopurile prelucrării**. După cum vom vedea în continuare, Împuternicitul poate răspunde (în solidar cu Operatorul) pentru acțiunile sale, în două situații: când încalcă instrucțiunile primite de la Operator, respectiv atunci când încalcă obligațiile pe care i le impune lui, ca împuternicit, GDPR.

Exemple utile pentru înțelegerea relației dintre operator și împuternicit

Exemple utile, pentru înțelegerea rolului Operatorului și Împuternicitului, dintre cele reținute de Opinia 1 din 2010 a Grupului de Lucru Articol 29, cu privire la conceptele de operator sau împuternicit, menționată anterior.

Marketingul prin poștă[3]

Întreprinderea ABC încheie contracte cu diferite organizații în vederea realizării campaniilor sale de marketing prin poștă. Aceasta oferă instrucțiuni clare (ce material de marketing trebuie trimis și cui trebuie trimis, cine trebuie plătit, ce sume, până la ce dată etc.). Deși organizațiile au o anumită libertate de decizie (inclusiv referitor la programul pe care să-l utilizeze), îndatoririle lor sunt destul de clar și de bine stabilite și, chiar dacă serviciul poștal ar putea da orientări (de exemplu, o recomandare împotriva trimiterii de mesaje publicitare în luna august), acestea acționează conform instrucțiunilor întreprinderii ABC.

[2] http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_ro.pdf
[3] Vezi pagina 13 din Opinia 1 din 2010. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_ro.pdf

Mai mult, o singură entitate, întreprinderea ABC, are dreptul să utilizeze datele prelucrate – toate celelalte entități trebuie să se bazeze pe temeiul juridic al întreprinderii ABC în cazul în care este investigată capacitatea lor legală de a prelucra datele. În acest caz, este evident că întreprinderea ABC are rolul de operator de date, iar fiecare dintre organizațiile separate poate fi considerată persoană împuternicită pentru prelucrarea datelor, cu privire la prelucrarea specifică a datelor pe care o realizează în numele său.

Monitorizarea secretă a angajaților[4]

Un membru al consiliului director al unei întreprinderi decide să monitorizeze în secret angajații întreprinderii, chiar dacă această decizie nu este susținută în mod oficial de consiliu. Întreprinderea ar trebui considerată operator, putând face obiectul posibilelor reclamații și răspunderii pe care o implică acest lucru în relație cu angajații săi, ale căror date cu caracter personal au fost utilizate abuziv. Răspunderea întreprinderii apare în special deoarece, în calitate de operator, aceasta are obligația de a asigura respectarea normelor de securitate și de confidențialitate. Utilizarea abuzivă de către un funcționar al întreprinderii sau de către un angajat ar putea fi considerată ca fiind rezultatul unor măsuri de securitate necorespunzătoare.

Aceasta, indiferent dacă, mai târziu, respectivul membru al consiliului director sau alte persoane fizice din cadrul întreprinderii ar putea fi, de asemenea, considerate răspunzătoare, atât din punct de vedere al dreptului civil – și față de întreprindere - cât și din punct de vedere al dreptului penal. Această situație poate apărea, de exemplu, dacă respectivul membru al consiliului director ar utiliza datele colectate în scopul obținerii unor favoruri personale din partea angajaților: el ar trebui considerat ca având rolul de „operator” și răspunzător pentru utilizarea acestor date.

Societăți de recrutare de personal[5]

Societatea Headhunterz Ltd ajută întreprinderea Enterprize Inc în recrutarea de personal. Contractul precizează în mod clar că „Headhunterz Ltd va acționa în numele întreprinderii Enterprize, iar în ceea ce privește prelucrarea datelor cu caracter personal, are rolul de persoană împuternicită pentru prelucrarea datelor. Enterprize este operatorul de date exclusiv”. Totuși, Headhunterz Ltd se află într-o poziție ambiguă: pe de o parte, aceasta are rolul de operator în raport cu persoanele aflate în căutarea unui loc de muncă, iar pe de altă parte își asumă rolul de persoană împuternicită care acționează în numele operatorilor, precum Enterprize Inc și alte întreprinderi care recrutează personal prin intermediul său.

În plus, Headhunterz – și renumitul său serviciu cu valoare adăugată „plasare a forței de muncă la nivel global” - caută candidați potriviți atât consultând CV-urile primite direct de Enterprize, cât și cele pe care le are deja în baza sa amplă de date. Astfel, societatea Headhunterz, care, conform contractului, este plătită numai pentru contractele efectiv semnate, crește probabilitatea de plasare a forței de muncă, sporindu-și astfel veniturile. Conform celor de mai sus, se poate concluziona că, în pofida calificării conform contractului, se consideră că Headhunterz Ltd are rolul de operator, controlând împreună cu întreprinderea Enterprize Inc cel puțin acele serii de operațiuni care se referă la recrutarea personalului pentru Enterprize.

[4] Vezi pagina 17 din Opinia nr. 1 din 2010
http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_ro.pdf

[5] Vezi pagina 19 din Opinia 1 din 2010. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_ro.pdf

Accesul neautorizat al unui angajat[6]

Un angajat al unei societăți ajunge să cunoască, în îndeplinirea sarcinilor sale, date personale pe care nu are dreptul să le acceseze. În acest caz, acest angajat ar trebui considerat „terț" în raport cu angajatorul său, cu toate consecințele și responsabilitățile aferente în termeni de legalitate a comunicării și prelucrării datelor.

Un contabil ori un auditor financiar sunt Operatori sau Împuterniciți?

Potrivit Opiniei nr. 1 din 2010 a Grupului de Lucru Articol 29, contabilii au mai multe tipuri de calități, în funcție de operațiunile pe care le întreprind.

Contabilii[7]

Calificarea contabililor poate varia în funcție de context. În cazul în care contabilii oferă servicii publicului general și micilor comercianți pe baza unor instrucțiuni foarte generale („pregătiți declarațiile mele de venit"), aceștia – la fel ca avocații care acționează în circumstanțe similare și din motive similare – vor avea rolul de operatori de date.

Totuși, atunci când contabilul este angajat de o firmă și trebuie să se supună instrucțiunilor detaliate ale conducerii firmei, cum ar fi realizarea unui audit detaliat, atunci acesta, dacă nu este un angajat permanent, va avea rolul de persoană împuternicită, având în vedere instrucțiunile clare și libertatea sa limitată de acțiune. Totuși, există o condiție majoră, și anume faptul că ,atunci când contabilii consideră că au detectat practici ilegale pe care sunt obligați să le raporteze, având în vedere obligațiile lor profesionale, aceștia acționează independent în calitate de operatori.

Autoritatea de Supraveghere din Marea Britanie are o perspectivă[8] și mai uspr de explicat asupra calificării contabilului, spre exemplu, în relatia cu clientul sau.

”O companie își externalizează serviciile de contabilitate. Atunci când acționează în numele clientului său, contabilul este operator, din perspectiva datelor personale cuprinse în registrele contabile. Acest lucru se întâmplă pentru că un contabil ori alt furnizor profesional de servicii acționează in baza unor obligații profesionale ce le impun să își asume responsabilitatea pentru datele personale pe care le prelucrează. Spre exemplu, dacă un contabil detectează activități ilegale în timpul activității sale, poate fi obligat să raporteze aceste activități către poliție ori alte autorități. Prin realizarea acestui lucru, contabilul în cauză nu acționează în baza unor instrucțiuni primite de la client, ci în concordanță cu obligațiile profesionale pe care le are, deci devine, prin urmare, operator pe acel tip de prelucrări.

Atunci când furnizorii de servicii profesionale prelucrează date în conformitate cu obligațiile lor profesionale, ei o să acționeze ca operatori și nu vor putea împărți ori pasa obligațiile lor către client, în acest context”.

[6] Vezi pagina 32 din Opinia 1 din 2010 a Grupului de Lucru Art. 29 http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_ro.pdf

[7] Vezi pagina 30 din Opinia 1 din 2010. http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_ro.pdf

[8] https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

In these cases, the client will not have sole data controller responsibility even though they initiated the work by asking for advice or commissioning a report. Responsibility also lies with the professional service provider itself because it determines what information to obtain and process in order to do the work and because it is answerable itself for the content. The use of a lawyer provides a good illustration of why providers of professional services are not usually just data processors. A client receives legal advice and, regardless of whether or not he chooses to follow the advice, would not ask the lawyer to make amendments to the original advice – the lawyer controls the detailed content of the advice. Lawyers would also have their own professional responsibilities in terms of record keeping, the confidentiality of communications and so forth. Again, this points towards lawyers and similar professional service providers being data controllers in their own right.

Persoana Vizată

Este acea persoană fizică ale cărei date sunt prelucrate. De reținut ideea de mai sus că persoana vizată este **o persoana fizică, în viață**.

Prin urmare, e de menționat că GDPR nu are în vedere date referitoare la persoane juridice (ex. număr de înregistrare de la registrul comerțului, Cod fiscal etc.). La fel, adresele de tipul office@firma.ro sau websiteurile companiilor nu sunt date cu caracter personal.

Pot exista, însă, situații, prin care aceste date, referitoare la persoane juridice, să fie date cu caracter personal cu privire la o persoana fizică. Spre exemplu, dacă pe hârtia despre care vorbeam mai sus, în capitolul dedicat definirii datelor cu caracter personal, pe lângă numărul 4.930 este scris și J-ul unei companii, cu mențiunea că e vorba despre statul de plată al acelei companii, atunci acele date, puse cap la cap, devin date cu caracter pesonal pentru persoana care are salariul acela din statul de plată al companiei cu acel J.

Ce trebuie avut în vedere înainte de a începe o operațiune de prelucrare?

Precizări privind pregătirea prelucrării datelor personale

Din perspectiva GDPR, prin prelucrare de date cu caracter personal se înțelege orice activitate care se încadrează între colectarea datelor și ștergerea/distrugerea acestora.

Pornind de la aceste concluzii, o desfășurare logică privind procesul de proiectare a operațiunilor de prelucrare presupune ca operatorul să răspundă la următoarele întrebări:

1. Care este scopul operațiunii de prelucrare?
2. Care sunt datele personale ce urmează sa fie prelucrate prin intermediul acestei operațiuni?
3. Care sunt categoriile de persoane vizate pe care le implica operațiunea de prelucrare?
4. Care este temeiul legal al operațiunii de prelucrare?
5. Care este perioada de retenție (de păstrare) a datelor cu caracter personal și pe ce se fundamentează stabilirea acesteia?
6. Se va realiza operațiunea de prelucrare direct și doar de către Operator sau va fi implicat și un împuternicit?

7. Care sunt măsurile de securitate care asigură o diminuare a riscului asupra drepturilor și libertăților persoanelor vizate?

Doar operatorul răspunde la aceste întrebări, nu și împuternicitul. Împuternicitul realizează prelucrările operatorului, așa cum le-a definit acesta.

În cazul în care societatea care oferă servicii de contabilitate, salarizare sau audit financiar este o persoană împuternicită, aceasta nu va răspunde la întrebările de mai sus pentru prelucrările pe care le face în numele unui client operator. În acest caz, societatea va prelua răspunsurile pe care clientul operator le dă cu privire la întrebările de mai sus. Cu alte cuvinte, prelucrarea operatorului va deveni, implicit, și prelucrarea persoanei împuternicite. În lipsa instrucțiunilor primite de la operator, împuternicitul nu ar efectua acele operațiuni, prin urmare răspunsurile sunt cele definite de operator. Împuternicitul îl poate asista, însă, pe operator, în definirea unora dintre răspunsuri (în special cele legate de mijloacele prelucrării, precum și de toate celelalte elemente de natura sa).

În cazul în care vorbim despre activități internalizate de contabilitate ori salarizare (cum ar fi, spre exemplu, cazul unor departamente *in-house* dedicate acestor activități), atunci operatorul va trebui să răspundă (iar departamentele specializate să îl ajute în formularea răspunsului) la toate întrebările de mai sus.

Înainte de a răspunde, însă, la aceste întrebări, operatorul va avea în vedere principiile de prelucrare a datelor cu caracter personal, așa cum sunt ele cuprinse în Regulament.

Principii de prelucrare a datelor cu caracter personal, conform GDPR

GDPR impune o serie de principii pentru prelucrarea datelor cu caracter personal. Art. 5 alin (1) al GDPR enumeră aceste principii și le transformă în piatra de temelie a oricărei operațiuni de prelucrare. Aceste principii sunt extrem de importante, pentru că ele sunt asimilate unor adevărate reguli fundamentale pe care trebuie să se bazeze orice prelucrare de date cu caracter personal.

Datele cu caracter personal sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);

Cu alte cuvinte, în calitate de operator/împuternicit trebuie să vă asigurați că:

- aveți temeiuri corecte pentru colectarea și utilizarea datelor cu caracter personal;
- nu utilizați datele în moduri care au efecte negative nejustificate asupra persoanelor în cauză;
- sunteți transparenți cu privire la modul în care intenționați să utilizați datele și să oferiți persoanelor respective o informare detaliată în momentul colectării datelor lor personale.

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri („limitări legate de scop”);

Cu alte cuvinte, în calitate de operator/împuternicit trebuie să vă asigurați, că:

- oferiți persoanelor vizate, în informarea prezentată la momentul colectării datelor lor personale, o trecere în revistă a scopurilor pentru care colectați fiecare categorie de date;

- nu schimbați scopul pentru care au fost colectate datele, fără informarea prealabilă a persoanelor vizate și parcurgerea tuturor pașilor tranzitorii necesari, atunci când e cazul (spre exemplu, dacă e nevoie să obțineți consimțământul persoanei vizate pentru această nouă prelucrare).

(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);

Cu alte cuvinte, e important să:

- colectați un număr de date nici mai mic și nici mai mare pentru atingerea scopului propus;
- nu colectați date pe principiul “nu se știe niciodată când vom avea nevoie de ele”.

(d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate”);

Cu alte cuvinte, atunci când prelucrați date:

- trebuie să verificați regulat exactitatea datelor prelucrate sau, dacă acest lucru nu e posibil,
- să puneți la dispoziția persoanelor vizate un mecanism prin intermediul căruia să își poată corecta, completa sau actualiza datele personale respective.

(e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele („limitări legate de stocare”), drept pentru care:

- nu stocați / prelucrați datele personale colectate pentru o perioadă mai mare de timp decât aceea necesară îndeplinirii scopului (la momentul colectării, în informare, va trebui să spuneți persoanei vizate pentru ce perioadă de timp, identificată sau identificabilă, se va face prelucrarea - respectați acele reguli);
- revizuiți periodic datele prelucrate, pentru a identifica ce date sunt prelucrate, care nu mai respecta principiul limitării perioadei de stocare și vor trebui, prin urmare, șterse ori anonimizate.

(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”).

E important să:

- luați măsuri tehnice și organizatorice necesare pentru a defini un grad sporit de securitate a prelucrării datelor în organizația dumneavoastră (principii și proceduri interne de gestionare a regulilor de securitate și incidentelor de securitate);
- stabiliți cine este responsabil, în organizația dumneavoastră, de implementarea, urmărirea și actualizarea politicilor de securitate și a proceselor de securitate;
- perfectați o serie de documente necesare pentru identificarea incidentelor de securitate, tratarea lor internă, notificarea acestora către Autoritatea de Supraveghere ori către persoanele vizate.

Exemple practice privind aplicarea principiilor de prelucrare

Înțelegerea și acceptarea principiilor de mai sus este foarte importantă. Iată câteva exemple în care aceste principii au impact asupra prelucrărilor de date realizate de dumneavoastră.

1. Un client va trimite absolut toate datele pe care le are, pentru că nu știe ce anume e nevoie pentru realizarea activității de contabilitate. Primiți, deci, o serie de date cu care nu doar că nu aveți ce face, dar pe care, fără să știe, clientul dumneavoastră (operator de date) le transmite cuiva care nu ar trebui să aibă acces la ele, generând astfel un incident de securitate.

   De aceea, spre exemplu, dacă e să ne uităm la principiile de mai sus, e important să privim lucrurile prin prisma ideii că, atunci când se realizează o prelucrare de date, acestea trebuie reduse la minimul necesar. Construiți-vă, deci, o serie de politici interne cu privire la tipul de date pe care îl solicitați de la clienți, atunci când vorbim despre anumite tipuri de activități.

   Își dorește clientul un serviciu de contabilitate? Atunci, în principiu, nu are de ce să vă trimită și emailurile sau numerele de telefon ale tuturor clienților săi. Dacă sunt precizate în factură, atunci lucrurile sunt evidente, pentru că nu puteți despărți factura în mai multe bucăți.

   Dacă, însă, exportul de date pe care îl primiți de la client are un conținut ce poate fi ajustat, construiți împreună cu clientul o politică menită să selecteze doar acele date care sunt absolut necesare pentru realizarea activității pe care v-ați asumat-o.

   Aveți nevoie de mai multe date privitoare la o anumită tranzacție ori privitoare la un anumit client? Puteți cere acele date, justificând cererea, dar le veți cere doar pentru clientul în cauză, nu pentru toți ceilalți clienți.

2. Bineînțeles, pentru activitatea de audit, lucrurile sunt mai simple sau mai complicate (după cum le privim). În teorie, cel puțin, un auditor ar trebui să aibă acces la absolut toate datele de care are nevoie pentru a-și desfășura activitatea. Prin urmare, e complicat de spus ce anume ar trebui limitat de către client.

   În același timp, însă, ideea centrală pe care se construiește un audit, din perspectiva activității de protecție a datelor cu caracter personal este aceea a “camerei de date”. Toate informațiile care sunt menite să fie analizate de către auditor vor fi “încărcate” într-un spațiu sigur, accesibil doar celor care au dreptul să vadă astfel de informații, cu posibilitatea de a se observa rapid accesul neautorizat la date.

3. Este vital, întotdeauna, să aveți construită, în interiorul companiei dumneavoastră, o politică de confidențialitate și un set de reguli foarte importante de urmat de către toți angajații, în privința activității de prelucrare de date cu caracter personal. În acest fel, reușiți să construiți un sistem care să respecte principiul confidențialității și integrității prelucrărilor. În capitolele următoare din acest ghid sunt redate câteva dintre măsurile importante care trebuie luate pentru a construi un cadru intern de respectare a prevederilor GDPR.

Conceptele *„privacy by design”* / *„privacy by default”*

Conceptele de “*privacy by design*” și “*privacy by default*” au fost aduse în prim plan de Ann Cavoukian, *Information & Privacy Commissioner* în provincia Ontario, Canada. În anii ‘90, Ann Cavoukian a definit 7 principii fundamentale pe baza cărora ar trebui desfășurate toate activitățile de prelucrare.

GDPR a preluat, într-o formă destul de apropiată de originalul Annei Cavoukian, principiile enunțate de aceasta și le-a transpus în două reguli importante.

1. *Privacy by Design* implică faptul că orice organizație care dorește să respecte GDPR va trebui să elaboreze politici, proceduri și sisteme care respectă Regulamentul, **chiar de la începutul dezvoltării produsului sau a proceselor sale de prelucrare**. Cu alte cuvinte, ideea de respectare a principiilor GDPR trebuie inclusă în chiar planurile de arhitectură ale viitoarelor activități de prelucrare.

2. *Privacy by Default* implică faptul că operatorii de date trebuie să pună în aplicare măsuri adecvate, atât la nivel tehnic, cât și organizațional, pentru a se asigura că datele cu caracter personal colectate sunt utilizate numai pentru scopul specific menționat. Aceasta înseamnă că **trebuie colectată cantitatea minimă necesară de date cu caracter personal, să se minimizeze prelucrarea și să se controleze stocarea și accesibilitatea acestora**.

Atunci când se concepe un proces de prelucrare de date, se are în vedere includerea acestor principii în schema de proces care se realizează. De asemenea, e foarte importantă documentarea (să se poata proba în viitor) faptului ca s-a avut în vedere atât ideea de *„privacy by desig”*, cât și ideea de *„privacy by default”* la momentul definirii unei activități de prelucrare.

Pregătirea prelucrării datelor personale

Operatorii vor întocmi un plan al prelucrării pe baza răspunsurilor la întrebările menționate la începutul capitolului:

Întrebarea 1: Care este scopul operațiunii de prelucrare?

Prin scop al prelucrării se înțelege acea finalitate pe care Operatorul o așteaptă de la prelucrarea în cauză. Plata salariilor este un scop al prelucrării. Realizarea auditului este un scop al prelucrării. Întocmirea dosarului de salariat este un alt scop.

E foarte importantă definirea cât mai corect cu putință a scopului prelucrării, pentru că de această definire depind, apoi, mai multe consecințe. În primul rând, fiecare astfel de prelucrare va implica o serie de date personale, va trebui fundamentată pe unul dintre cele 6 variante de temeiuri legale și va implica o anumită perioadă de retenție a datelor.

Apoi, în cazul în care datele cu caracter personal sunt prelucrate într-un alt scop decât cel pentru care acestea au fost colectate, va trebui să se furnizeze persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și alte informații necesare.

Întrebarea 2: Care sunt datele personale ce urmează sa fie prelucrate prin intermediul acestei operațiuni?

Imediat ce se definește scopul unei prelucrări, e relativ usor să se definească și tipul de date cu caracter personal care vor fi incluse în prelucrarea în cauză. Cu alte cuvinte, să spunem că prelucrarea vizează întocmirea registrului general de evidență a salariaților (REVISAL).

Potrivit art. 3 al Hotararii Guvernului nr. 500 din 2011, privind registrul general de evidență a salariaților, registrul privat se completează în ordinea încheierii contractelor individuale de muncă și cuprinde o serie de elemente obligatorii, printre care amintim:

- elementele de identificare ale tuturor salariaților: numele, prenumele, codul numeric personal - CNP, cetățenia și țara de proveniență,
- funcția/ocupația,
- datele din actele de studii de lungă durată ale persoanei, precum și
- datele privitoare la profilul/specializarea/calificarea, conform actelor/certificatelor de calificare,
- salariul de bază lunar brut și sporurile, astfel cum sunt prevăzute în contractul individual de muncă,
- Etc.

Prin urmare, dacă vorbim despre operațiunea de prelucrare al cărei scop este întocmirea registrului privat de evidență a salariaților, atunci scopul va fi "întocmirea registrului privat de evidență a salariaților", iar datele prelucrate vor fi cele precizate în HG 500/2011.

Este important, ori de câte ori se stabilește o operațiune de prelucrare, să se specifice clar care este scopul acesteia și care sunt datele personale pe care le implică aceasta operațiune de prelucrare.

În cadrul mai multor operațiuni de prelucrare ar putea fi utilizate aceleași categorii de date cu caracter personal. Spre exemplu, în cadrul unei companii, numele persoanei vizate va fi utilizat atât în operațiunea care implică realizarea registrului privat de evidență a salariaților, cât și în operațiunea care implică plata salariilor, cât și în operațiunea care implică acordarea unor concedii medicale etc.

Exemple practice

Potrivit Opiniei Grupului de Lucru art. 29, nr. 2 din 2017, privind prelucrarea datelor la locul de muncă, ar trebui avute în vedere mai multe aspecte practice, atunci când analizăm aceste prelucrări. Iată câteva situații menționate în această Opinie[9].

Operațiunile de prelucrare în timpul procesului de recrutare

Utilizarea platformelor de comunicare socială de către persoane este larg răspândită, iar posibilitatea de vizualizare publică a profilurilor de utilizator în funcție de setările alese de către titularul de cont este o situație relativ frecventă. Prin urmare, angajatorii ar putea crede că verificarea profilurilor sociale ale unor candidați în perspectivă poate fi justificată în cadrul proceselor lor de recrutare. Acest lucru poate fi valabil și în cazul altor informații publice despre un potențial angajat.

[9] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

Însă angajatorii nu ar trebui să presupună că, doar datorită faptului că profilul unei persoane de pe platformele de comunicare socială este public, aceștia sunt autorizați să prelucreze respectivele date în scopuri proprii. Este nevoie de un temei juridic pentru o astfel de prelucrare, cum ar fi interesul legitim.

În acest context, înainte de verificarea unui profil de pe platformele de comunicare socială, angajatorul trebuie să aibă în vedere dacă profilul candidatului de pe respectivele platforme este legat de un context profesional sau personal, deoarece acest lucru poate fi un element important care indică admisibilitatea juridică a inspecției datelor. În plus, angajatorii sunt autorizați să colecteze și să prelucreze datele cu caracter personal referitoare la candidații la un post doar în măsura în care colectarea acestor date este necesar și relevantă pentru îndeplinirea atribuțiilor postului pentru care aceștia s-au înscris.

Datele colectate în timpul procesului de recrutare ar trebui să fie, în general, șterse de îndată ce devine evident faptul că nu va fi înaintată o ofertă de muncă sau că aceasta nu este acceptată de către persoana în cauză. De asemenea, persoana trebuie să fie corect informată cu privire la orice astfel de prelucrare înainte de a se angaja în procesul de recrutare.

Nu există niciun temei juridic pentru ca un angajator să solicite unui potențial angajat să „devină prieten” cu potențialul angajator sau să obțină accesul în alte moduri la conținutul profilului acestuia.

Operațiunile de prelucrare care rezultă din prelucrarea după angajare

Dat fiind că există profiluri pe platformele de comunicare socială și că au fost dezvoltate noi tehnologii analitice, angajatorii au (sau pot obține) capacitatea tehnică de a verifica permanent angajații, colectând informații referitoare la prietenii, opiniile, convingerile, interesele, obiceiurile, locația, atitudinile și comportamentele acestora și captând așadar date, inclusiv date sensibile, legate de viața privată și de familie a angajatului.

Verificarea după angajare a profilurilor angajaților pe platformele de comunicare socială nu ar trebui să fie generalizată. Mai mult, angajatorii ar trebui să se abțină de la a solicita unui angajat sau candidat la un post accesul la informații pe care acesta le partajează cu alte persoane prin socializarea în rețea.

În plus, nu ar trebui să li se impună angajaților să utilizeze un profil pe platformele de comunicare socială pus la dispoziție de către angajatorul lor. Chiar și atunci când acest lucru este prevăzut în mod specific în contextul sarcinilor acestora (de exemplu, purtător de cuvânt al unei organizații), aceștia trebuie să își rezerve opțiunea de a-și crea un profil care nu este public, „în afara serviciului”, pe care să îl poată folosi în locul profilului „oficial” asociat angajatorului, iar acest lucru ar trebui specificat în termenii și condițiile contractului de muncă.

Operațiunile de prelucrare legate de timp și de prezență

Sistemele care permit angajatorilor să controleze cine poate intra în sediile lor și/sau în anumite zone din sediile lor pot permite, de asemenea, urmărirea activităților angajaților.

Deși astfel de sisteme există de mai mulți ani, noile tehnologii destinate monitorizării timpului și prezenței angajaților sunt utilizate din ce în ce mai mult, inclusiv cele care prelucrează date biometrice, și altele, precum cele de urmărire a dispozitivelor mobile.

Chiar dacă astfel de sisteme pot constitui o componentă importantă a pistei de audit a unui angajator, ele prezintă totodată riscul de a asigura un nivel invaziv de cunoștințe și de control în ceea ce privește activitățile angajatului atunci când se află la locul de muncă.

Pentru mai multe astfel de exemple, este utilă parcurgerea Opiniei[10] nr. 2 din 2017, a Grupului de Lucru Art. 29, privind prelucrarea de date personale la locul de muncă. Această Opinie lămurește multe dintre aspectele legate de monitorizarea angajaților, montarea unor dispozitive pe mașinile acestora etc.

Întrebarea 3: Care sunt categoriile de persoane vizate pe care le implică operațiunea de prelucrare?

Persoanele vizate în operațiunile de prelucrare pe care le implică muncă unui contabil, expert contabil sau auditor financiar sunt reprezentate de angajații potențiali sau actuali ai unei companii, precum și clientii acelei companii. Într-o mai mică măsură, prelucrarea datelor de către contabil sau auditorul financiar implică și administratorul, acționarii sau asociații unor companii.

Întrebarea 4: Care este temeiul legal al prelucrării?

Potrivit GDPR (art. 6 alin (1)), prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

(a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

(b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

(d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

(e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Enumerarea de mai sus nu e un top și nici o prezentare prioritară a acestor condiții. Un operator trebuie să aibă la baza activității sale de prelucrare unul dintre punctele de mai sus. Pentru majoritatea operatorilor (excludem entitățile publice și alte tipuri de entități extrem de specifice), cele patru condiții de reținut (denumite și temeiuri ale prelucrării) sunt:

- Existența unei obligații legale a operatorului;
- Executarea unui contract / demersuri înainte de încheierea unui contract;

[10] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

- Existența unui interes legitim al operatorului sau al unei terțe părți;
- Consimțământul persoanei vizate.

Întotdeauna, înainte de a începe o operațiune de prelucrare, trebuie analizat și documentat (analiza trebuie să poată fi probată ulterior) temeiul prelucrării ca fiind unul dintre punctele enumerate mai sus. Fără existența unui temei justificat, prelucrarea nu este legală.

Practic, trebuie să se parcurgă un șir logic de întrebări care ar putea să lămurească temeiul existent pentru un anumit tip de prelucrare.

4.1 Am o obligație legală sa fac acea prelucrare?

Dacă ne referim la exemplul de mai sus, al registrului privat de evidență a salariaților, răspunsul e simplu. Hotarârea Guvernului nr. 500/2011 impune aceasta obligație. Prin urmare, temeiul operațiunii de prelucrare e unui clar - obligația legală impusă prin Hotarârea Guvernului nr. 500/2011. Dar situațiile în care legea ne impune sa realizăm un anumit tip de prelucrare nu trebuie văzute doar în legatură directă cu contractul de muncă.

Spre exemplu, GDPR impune tuturor operatorilor să mențină un registru al cererilor formulate de persoanele vizate, în virtutea drepturilor pe care le au, conform GDPR. Cu alte cuvinte, dacă o persoana vizată cere ștergerea datelor sale din sistemele operatorului, operatorul va trebui să menționeze această cerere într-un registru. Printre altele, în registru va fi menționat deci tipul de cerere (ștergere, în cazul nostru), dar vor apărea și datele persoanei care a cerut ștergerea (așa cum e ea identificată în sistemul operatorului - prin email sau nume / serie de buletin), dar și alte detalii legate de această cerere.

În final, trebuie explicat că obligația legală nu există doar atunci când o lege românească impune realizarea unui anumit tip de prelucrare, ci și atunci când prelucrarea în cauză este impusă prin intermediul dreptului Uniunii. Dreptul Uniunii Europene este format din legislația primară (Tratatele UE) și legislația secundară (regulamentele, directivele şi deciziile care derivă din principiile şi obiectivele stabilite prin Tratate).

Există, însă, operațiuni de prelucrare ce nu sunt impuse prin lege. În cazul acelor operațiuni de prelucrare, va trebui să trecem la următoarele temeiuri prevăzute de GDPR, să vedem care e aplicabil. Trecem, deci, la întrebarea următoare.

4.2 Există un contract care urmează sa fie semnat cu persoana vizată? Dar un contract ce e deja în aplicare există?

Cu alte cuvinte, întrebarea a doua vizează existența unui contract (potențial sau existent) cu persoana vizată, care să impună realizarea acelei prelucrări de date cu caracter personal.

Atunci când vorbește despre temeiul **contract,** GDPR se referă la două situații potențiale:

1. Pașii anteriori intrării într-un contract, la cererea persoanei vizate (“demersuri la cererea persoanei vizate înainte de încheierea unui contract”, în accepțiunea Regulamentului);
2. Executarea unui contract.

Exemple:

Trimiterea de CV-uri de către persoanele vizate ca urmare a ofertei de job-uri a unei companii

În cazul în care compania X pune pe siteul său web un anunț privind un job, iar Ion Popescu trimite către compania X CV-ul său, pentru că își dorește să fie angajat în cadrul acelei companii, pe acel post, vorbim despre situația de la punctul 1 de mai sus. Cu alte cuvinte, Ion Popescu a inițiat discuția cu compania X. A fost un demers pe care l-a pornit el, înainte de încheierea unui contract la care s-ar putea ajunge, dacă se va dovedi potrivit pentru acea slujbă.

Aici, vorbim deci despre o prelucrare care se face în temeiul "contract", mai exact "demersuri la cererea persoanei vizate înainte de încheierea unui contract".

Plata celui de-al 13-lea salariu al unui angajat

Este genul de obligație prevazută în contractul de muncă dintre angajat și angajator. Ca urmare a contractului, angajatorul va trebui să îi prelucreze angajatului, spre exemplu, Numele, Prenumele și IBAN-ul pentru a-i putea face plata salariului prin bancă. E un alt exemplu în care temeiul care ar putea fi folosit de angajator este "contractul", mai precis "executarea contractului".

Există, însă, situații în care prelucrarea nu e impusă prin intermediul legislației naționale ori prin intermediul dreptului Uniunii și nici nu există un contract cu persoana vizată, în curs de semnare sau în curs de executare. Va trebui, deci, să mergem mai departe cu întrebările.

4.3 Să fie nevoie, oare, de consimțământul persoanei vizate?

Ar fi bine ca acest temei să fie lăsat cât mai spre final, atunci când se analizează temeiurile aplicabile unui anumit tip de prelucrare. De regulă, există momente în care consimțământul este obligatoriu (ex. realizarea de campanii de marketing direct în mediul electronic, plasarea, scrierea și citirea cookie-urilor pe terminalul abonaților etc.) și momente în care consimțământul este una dintre opțiunile de temei util pentru prelucrare (prelucrarea datelor sensibile (date de sănătate, date genetice etc.), realizarea de decizii automatizate, inclusiv ca urmare a profilării, cu efecte juridice sau similar semnificative).

În privința folosirii consimțământului în relația dintre angajați și angajatori, potrivit Opiniei nr. 2 din 2017, a Grupului de Lucru Art. 29 privind prelucrarea datelor personale la locul de muncă, "angajații nu sunt aproape niciodată în măsură să își exprime, să refuze sau să își revoce în mod liber consimțământul, având în vedere dependența care rezultă din relația dintre angajator și angajat. Având în vedere dezechilibrul de puteri, angajații își pot da consimțământul liber numai în situații excepționale, atunci când nu există deloc consecințe legate de acceptarea sau respingerea unei oferte". Angajatorii ar trebui să nu folosească consimțământul drept temei atunci când vorbim despre o prelucrare de date de la locul de muncă pentru că acel temei ar putea fi invalidat în diferite circumstanțe de instanță ori de Autoritatea de Supraveghere.

În plus, efectele pe care le are consimțământul nu sunt întotdeauna potrivite pentru anumite prelucrări. Spre exemplu, dacă alegi gresit, te poti afla în situația în care ai putea să-ți bazezi o prelucrare pe consimțământul persoanei vizate, iar apoi să te trezești că, dacă persoana vizată alege să-și retragă consimțământul, vei fi pus în fața unei situații foarte ciudate: va trebui să ștergi datele și să încetezi prelucrarea. Or, în anumite contexte, acest lucru te va expune unor probleme extrem de serioase.

Ipoteza prelucrării datelor personale ale unui angajat în virtutea temeiului "consimțământ"

În cazul ipotezei unui angajat, pentru prelucrarea datelor căruia, în loc să te bazezi pe obligația legală de prelucrare (cum e cazul datelor incluse în registrul de evidență a salariaților) sau pe executarea unui contract (cum e cazul altor prelucrări din categoria celor legate de contractul de muncă), alegi să te bazezi pe consimțământ. Ignorăm, mergând spre absurd, ce spune Grupul de Lucru (că în relațiile de muncă nu e bine să te bazezi pe consimțământ atunci când faci prelucrarea) și considerăm că ne-am putea baza pe consimțământ.

Ce s-ar întâmpla dacă acel angajat ar veni să-și retragă consimțământul? Pentru că, potrivit art. 7 alin (3) al GDPR, **persoana vizată are dreptul să își retragă în orice moment consimțământul**. Mai mult, retragerea consimțământului are drept urmare obligația de a înceta prelucrarea și de a șterge / distruge datele în cauză. Cum poate cineva să șteargă din registrul de evidență a salariaților, din dosarul de personal ori contractul de muncă al unui angajat? Realitatea e că nu poate. Și, în acest caz, se va dovedi faptul că alegerea consimțământului drept temei pentru prelucrare nu a fost cea mai inspirată idee.

Totuși, dacă pentru anumite tipuri de prelucrare este nevoie să se obțină consimțământul de la o persoană vizată pentru prelucrarea datelor sale cu caracter personal, trebuie să se asigure obținerea consimțământului:

(a) liber exprimat, expres, informat și clar; și

(b) printr-o declarație clară de consimțământ sau o acțiune afirmativă clară care demonstrează consimțământul.

Trebuie ca și retragerea consimțământului să se poate efectua la fel de ușor ca și acordarea acestuia și trebuie comunicat persoanei vizate acest drept.

Sub GDPR, consimțământul nu mai este implicit (trebuie să existe o acțiune pozitivă și clară).

Aspecte practice

În practică, mecanismele de obținere a consimțământului trebuie să respecte următoarele cerințe:

Cerință	Ce înseamnă

Liber exprimat	Personale vizate nu trebuie forțate să ofere consimțământul, altfel acesta este invalid. De exemplu, consimțământul nu trebuie să fie o condiție pentru înscrierea la un serviciu decât dacă este absolut necesar pentru acel serviciu (de exemplu, când se bazează pe verificarea vârstei sau dacă localizarea este necesară pentru funcționarea corespunzătoare a unei aplicații). Consimțământul presupune că persoana vizată are cu adevărat o opțiune și că poți să îi oferi opțiunea de a spune nu. În cazul în care compania poate realiza aceste procesări și fără consimțământ, atunci nu acesta este temeiul legal potrivit (de ex., sistemele CCTV).
Expres	Consimțământul trebuie obținut pentru fiecare tip de prelucrare pe care vrei să o faci și este legat expres de organizațiile care se vor baza pe acesta. Consimțământul trebuie să fie granular dacă este luat pentru multiple operațiuni. De asemenea, dacă consimțământul este cerut pentru terți (care nu sunt împuterniciți ai companiei), acesta trebuie obținut indicând numele terțului.
Informat	Persoanelor vizate trebuie să li se ofere informații ample (sub forma unei notificări corecte de prelucrare) asupra naturii și scopului prelucrării, pentru care își dau consimțământul. Acea informație trebuie să conțină detalii despre organizațiile (inclusiv terții) care se bazează pe consimțământ și aceste organizații trebuie numite în momentul obținerii consimțământului.
Clar	Cererile pentru consimțământ trebuie separate de alți termeni și condiții pentru a asigura lipsa oricui dubiu privind acordarea consimțământului.
Include o declarație clară de consimțire sau o acțiune pozitivă clară demonstrând consimțământul.	Pentru un consimțământ valid, trebuie să existe o acțiune pozitivă și clară, precum bifa unei casete sau realizarea unui anumit pas care se constituie într-o acțiune relevantă. Căsuțele "*pre-ticked*" sau "*opt-out*" nu sunt suficiente pentru a indica consimțământul și nu trebuie folosite!

Ușor de retras	Personale vizate trebuie să fie conștiente că pot retrage consimțământul oricând și trebuie să primească informațiile despre cum pot face asta. Trebuie să fie la fel de simplu să retragi consimțământul ca și să îl oferi. Deci trebuie să existe mecanisme simple pentru a retrage consimțământul.

Demonstrarea conformării

Pentru a demonstra conformitatea cu cerințele de consimțământ, trebuie păstrate înregistrări care să demonstreze că persoanele vizate și-au dat consimțământul, inclusiv informațiile care le-au fost oferite la primirea acestuia și când și cum și-au dat consimțământul.

Mergând mai departe cu firul logic al întrebărilor, să spunem că, în cazul prelucrării despre care vorbim, nu este aplicabil nici consimțământul, ca temei legal, pentru că e o prelucrare din sfera relațiilor de muncă ori nu ne aflăm în alt caz în care, prin GDPR ori lege specială, ar trebui să obținem consimțământul persoanei vizate pentru efectuarea prelucrării. Ajungem, deci, la următoarea întrebare.

4.4 Are compania un interes legitim ori are o terță parte un interes legitim să realizeze acea prelucrare?

Răspunsul simplu ar fi că, aproape întotdeauna, o companie are un interes legitim să realizeze prelucrări ale unor date personale. Ce este un interes legitim? Este acel tip de interes care nu e contrar legii. Cu alte cuvinte, o companie are un interes legitim să își crească afacerea, să crească performanțele angajaților săi, să își monitorizeze bunurile, să monitorizeze accesul în anumite incinte ale sale etc. Toate aceste scopuri de prelucrare ar fi interese legitime ale companiei respective.

Exemple utile

Operatorii care fac parte dintr-un grup de întreprinderi sau instituții afiliate unui organism central pot avea un interes legitim de a transmite date cu caracter personal în cadrul grupului de întreprinderi în scopuri administrative interne, inclusiv în scopul prelucrării datelor cu caracter personal ale clienților sau angajaților.

Cu alte cuvinte, atunci când o companie trimite date către alte companii din grup, în state din Zona Economica Europeană, pentru că salarizarea ori contabilitatea sunt ținute la nivel de grup, atunci temeiul pentru o astfel de prelucrare ar putea fi interesul legitim al companiei.

Prelucrarea datelor cu caracter personal în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor, precum și securitatea serviciilor conexe oferite de aceste rețele și sisteme sau accesibile prin intermediul acestora, de către autoritățile publice, echipele de intervenție în caz de urgență informatică, echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de rețele și servicii de comunicații electronice, precum și de către furnizorii de servicii și tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză.

Pentru a fi valid, interesul legitim trebuie să îndeplinească mai multe condiții, asa cum reies acestea din preambulul 47 al GDPR:

1. Prelucrarea trebuie să fie necesară pentru îndeplinirea scopului.

2. Scopul trebuie să fie un interes legitim al operatorului ori al unei terțe părți.
3. Acel interes legitim să nu fie mai presus de interesele, drepturile și libertățile fundamentale ale persoanei vizate. Cu alte cuvinte, atunci când alegem interesul legitim, trebuie parcurs așa-numitul test al "balansării intereselor" operatorului și persoanei vizate.

Această analiză, dacă interesul legitim al operatorului este mai presus de interesele persoanei vizate, se poate face luând în considerare așteptările rezonabile ale persoanelor vizate, așteptări bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. Cu alte cuvinte, mai degrabă poți avea un interes legitim cu privire la un anumit tip de prelucrare a datelor clienților sau angajaților, decât să ai un interes legitim asupra unui anumit tip de prelucrare a datelor unor terți cu care nu ai legătură.

Consecința directă a utilizării interesului legitim ca temei al unei prelucrări este posibilitatea persoanei vizate de a obiecta la prelucrarea în cauză. Dacă persoana vizată obiectează (dreptul respectiv trebuie menționat în informarea oferită persoanei vizate), atunci operatorul va trebui să personalizeze analiza interesului legitim, inclusiv acel test al balansării intereselor, la situația particulară a respectivei persoane vizate. Ulterior, dacă în urma acestei analize va reieși că interesele operatorului prevalează (adică sunt mai presus), poate continua prelucrarea. Dacă, în schimb, va descoperi că obiecțiunea persoanei vizate este justificată, operatorul va trebui să înceteze prelucrarea.

Întrebarea 5: Care este perioada de retenție a datelor cu caracter personal și pe ce se fundamentează stabilirea acesteia?

Articolul 5, alin (1) lit e) al GDPR menționează că "Datele cu caracter personal sunt [...] **păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele**; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate (limitări legate de stocare)".

Mai mult, în preambulul (39) al GDPR se vorbește despre "asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum", precum și de faptul că "în vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuirea periodică".

Prin urmare, ori de câte ori se realizează o operațiune de prelucrare, trebuie menționată foarte clar perioada pentru care se vor stoca datele în cauză, iar aceasta perioadă nu trebuie să fie mai mare decât perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele.

Singura excepție o constituie stocarea datelor în vederea prelucrării exclusiv în scopuri:

- de arhivare în interes public,
- de cercetare științifică sau istorică,
- statistice,

- și doar sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în Regulament în vederea garantării securității acestor date.

GDPR nu cuprinde, în textul său, perioade pentru care trebuie stocate datele în anumite tipuri de prelucrare. Aceste perioade trebuie stabilite de Operator:

- fie în urma unei analize practice a situației (nu se stochează e-mailurile unor persoane, colectate pentru trimiterea de comunicări comerciale, pentru zeci de ani, dacă omul în sine nu a reacționat niciodată la e-mailurile operatorului, spre exemplu).
- fie prin respectarea unor obligații legale, care impun anumite termene de păstrare a unor documente (și, implicit, a datelor prelucrate prin intermediul realizării acelor documente) fiscale, din legislația muncii etc.

Exemple practice

Ordinul Ministerului Finanţelor Publice (MFP) nr. 2634/2015, în vigoare de la 1 ianuarie 2016, care stabileste documentele financiar-contabile care se păstrează timp de 5 ani, cu începere de la data încheierii exercițiului financiar în cursul căruia au fost întocmite: notă de recepție și constatare de diferențe, bon de consum, fișă de magazie, listă de inventariere, chitanță, dispoziție de plată/încasare către casierie, borderou de achiziție, borderou de achiziție (de la producători individuali), ordin de deplasare (delegație), ordin de deplasare (delegație) în străinătate (transporturi internaționale), decont de cheltuieli (pentru deplasări externe), decizie de imputare, etc.

Art. 25 din Legea contabilitatii, nr. 82 din 1991 prevede că “Registrele de contabilitate obligatorii şi documentele justificative care stau la baza înregistrărilor în contabilitatea financiară se păstrează în arhiva persoanelor prevăzute la art. 1 [ex. societăți comerciale – n.a.] timp de 10 ani, cu începere de la data încheierii exerciţiului financiar în cursul căruia au fost întocmite, cu excepţia statelor de salarii, care se păstrează timp de 50 de ani”.

Întrebarea 6: Se va realiza operațiunea de prelucrare direct și doar de către Operator sau va fi implicat și un împuternicit?

Acesta este unul dintre răspunsurile relativ simple. După cum se va observa mai departe, în capitolul dedicat relației dintre operator și împuternicit, e importantă această distincție pentru că ea ajută atât la construcția unui contract (acord privind prelucrarea datelor) corect între cele două părți, cât și la distribuirea responsabilității pe care părțile o au în fata Autorității de Supraveghere ori în fața persoanelor vizate.

Merită amintită, totuși, Opinia 1 din 2010 privind conceptele de operator și de împuternicit, care definește o serie de criterii care ajută în determinarea rolului părților, din acest punct de vedere:

- nivelul de instrucțiuni pe care îl dă operatorul, care determină gradul de independență pe care îl are împuternicitul față de operator.
- monitorizarea îndeaproape, de către operator, a execuției operațiunilor de prelucrare, poate sugera că acea parte este în controlul absolut al prelucrării.
- vizibilitatea pe care un operator o proiectează asupra persoanelor vizate poate crea așteptări în mintea acestora.

În toate cazurile, înainte de începerea unei operațiuni de prelucrare, trebuie decis dacă acea operațiune se va realiza în calitate de operator sau în calitate de împuternicit (o altă companie/entitate este

operator, către care se prestează serviciul în cauză – contabilitate, salarizare etc.). În primele capitole ale acestui document am amintit câteva situații practice prin care se poate deduce cum se poziționează contabilii în relația cu clienții, din această perspectivă.

Întrebarea 7: Care sunt măsurile de securitate care asigură o diminuare a riscului asupra drepturilor si libertăților persoanelor vizate?

Potrivit art. (5), alin (1) lit f) din GDPR, "Datele cu caracter personal trebuie [...] prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare".

GDPR amintește, în mod repetat, atunci când se vorbește despre securitatea prelucărilor, despre măsuri tehnice și organizatorice pe care trebuie să le implementeze atât operatorul, cât și împuternicitul.

Simplist vorbind, măsurile organizatorice sunt acțiuni prin intermediul cărora, în cadrul entității care prelucrează date, se creează politici, proceduri și mecanisme interne de organizare menite să asigure securitatea prelucrării.

Spre exemplu, prin măsuri organizatorice am putea aminti:

- training-ul personalului intern;
- politici interne de securitate (simplul fapt ca există o politică internă este un mecanism de securitate);
- asigurarea accesului în clădire/birou/camere/dulapuri doar pentru persoanele care au dreptul să fie acolo.

Măsurile tehnice au legătură cu capacitățile tehnologice pe care le presupune o astfel de prelucrare. Exemple de astfel de măsuri ar putea fi ideea că operatorul și împuternicitul trebuie să includă în arhitectura sistemelor informatice și:

a. soluții de tip *network intrusion*/*network protection* care să protejeze corespunzător toate sistemele ce conțin datele companiei ce sunt accesibile din internet sau alte rețele publice;
b. soluții de limitare a atacurilor de tip "brute-force", prin blocarea accesului de la surse pentru care s-au înregistrat tentative eșuate repetate de autentificare în sistem sau aplicație (ex. mai mult de 5 (cinci) autentificări eșuate în ultimele 5 (cinci) minute);

Vom discuta mai jos, la secțiunea dedicată incidentelor de securitate, despre ce alte lucruri ar trebui să facă operatorul și împuternicitul pentru a respecta cerintele GDPR în contextul asigurării securității prelucrărilor.

Cereri ce pot fi primite de la persoane fizice ale căror date le prelucrezi

Cererile vor fi analizate de companie în calitate de operator de date personale având în vedere răspunsurile la întrebările următoare:

Care sunt drepturile persoanelor vizate și ce implicații au aceste drepturi asupra companiei?

Privit ca ansamblu de reguli referitoare la protecția datelor cu caracter personal, GDPR pune în centrul său drepturile și libertățile persoanelor vizate. Pentru ca aceste drepturi și libertăți să fie respectate, Regulamentul obligă organizațiile (companii, autorități publice etc.) să aplice o serie de proceduri birocratice de natură să le determine să înțeleagă și să poată răspunde în timp util solicitărilor primite de la persoanele vizate ori de la Autoritățile de Supraveghere.

Avand în vedere că nu amenzile ar trebui să producă panică, ci realitatea dură, când persoanele vizate vor utiliza drepturile pe care le au pentru **a solicita accesul, ștergerea ori rectificarea datelor lor**, urmând ca, la aceste solicitări, să se dea un răspuns într-un termen impus de GDPR. Dacă estimăm numărul cererilor și asociem această realitate cu faptul că, datele pot fi răspândite între mai multe baze de date, sisteme de referință sau metode de stocare, putem aprecia adevărata imagine a provocărilor GDPR.

În cât timp trebuie să răspunzi la cererile persoanelor vizate?

În cadrul organizației, în calitate de operator, trebuie să se realizeze instruiri care să permită echipei să identifice și să știe unde trebuie direcționate toate aceste solicitări primite de la persoanele vizate.

Potrivit art. 12 din GDPR, compania în calitate de operator furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul articolelor 15-22 (dreptul de acces la date, dreptul de ștergere a datelor, dreptul la rectificarea datelor, dreptul de restricționare a datelor, dreptul la opoziție, dreptul la portabilitatea datelor), fără întârzieri nejustificate și în orice caz **în cel mult o lună de la primirea cererii.**

Această perioadă **poate fi prelungită cu două luni** atunci când este necesar, dar operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii.

În cazul în care operatorul nu ia măsuri cu privire la cererea persoanei vizate, acesta va informa persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.

Pasul obligatoriu, înainte de răspunsul la cererea persoanei vizate: identificarea persoanei vizate

E foarte important, însă, ca persoana vizată să fie identificată corect înainte de a i se furniza răspunsul la cererile sale. Identificarea trebuie să aibă în vedere, atunci când e cazul, inclusiv solicitarea de informații suplimentare, menite să ajute operatorul să identifice persoana vizată în sistemul său de referință.

Exemplu

Ion Popescu trimite către compania SC Denumire SRL o cerere de acces la datele sale personale. Cererea este trimisă pe email și e formulată foarte simplu: "aș dori să știu toate datele mele personale pe care le prelucrați dumneavoastră". Cererea este înregistrată la registratura SC Denumire SRL pe data de 1 martie 2018. Potrivit GDPR, compania va avea o lună pentru a da un răspuns cererii formulate de Ion Popescu.

Compania a implementat însă un sistem automatizat, prin care datele prelucrate să fie identificate, alături de scopul, temeiul prelucrării, precum și alte informații utile asociate acestora, iar răspunsul la cererile persoanelor vizate să fie furnizat automat. Însă, pentru a putea furniza răspunsul, compania are nevoie să identifice corect persoana vizată. Îi cere informații care o ajută să facă identificarea în mod corect.

Apoi, în funcție de rezultatele identificării, pot apărea mai multe variante de răspuns:

1. Identificarea e corect realizată, răspunsul se trimite automat în interiorul termenului de o lună impus de GDPR.

2. Identificarea e corect realizată, dar e nevoie de eforturi suplimentare pentru a compila un răspuns. I se răspunde, totuși, persoanei vizate, în interiorul termenului de 1 lună, cu menționarea faptului că e nevoie de timp suplimentar (ex. încă 45 de zile) pentru a furniza informațiile solicitate. În același răspuns, i se explică persoanei vizate că poate depune o plângere la Autoritatea de Supraveghere, dacă nu e mulțumită de acest răspuns.

3. Identificarea nu se poate face. Persoanei vizate i se furnizează un răspuns în interiorul termenului de 1 lună (sau de 1 lună + x zile prelungire), i se explică faptul că, din anumite motive, nu s-a putut face identificarea și că nu se poate, prin urmare, furniza un răspuns la solicitare. În același răspuns i se menționează persoanei vizate ideea că poate face o plângere la Autoritatea de Supraveghere, dacă va considera necesar.

Au aceste cereri o formă standard?

Cererile formulate de persoanele vizate **nu trebuie să aibă o formă standard,** nu trebuie să fie completate folosind un șablon ori un tipizat. Ele pot veni pe orice fel de canal (verbal, electronic, prin telefon, poștă scrisă, facebook, messenger), în orice formă ar fi ele formulate (în limbaj obișnuit, în limbaj academic, juridic etc.).

GDPR nu conține prevederi speciale în acest sens. La alin (3) al art. 12, GDPR menționează doar că "În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format".

Răspunsul la astfel de cereri trebuie formulat folosind o metodă care să poată fi probată ulterior. Cu alte cuvinte, trebuie **formulat în scris (inclusiv în formă electronică) și trebuie inclus într-o bază**

sistematizată de răspunsuri, pentru a putea fi regăsit mai ușor în viitor, atunci când va fi nevoie de acest lucru.

Mai mult, includerea răspunsurilor într-o evidență sistematizată este utilă pentru documentarea cazurilor în care aceste solicitări de la persoanele vizate au un caracter vădit abuziv sau repetitiv, asa cum se tratează în capitolul următor.

Răspunsul trebuie să fie gratuit sau poate fi oferit și pe bani?

Regula principală impusă de GDPR este aceea că răspunsul la cererile persoanelor vizate, precum și informarea persoanelor vizate trebuie să se realizeze gratuit. Art. 12 alin (5) al GDPR menționează expres faptul că "informațiile furnizate în temeiul articolelor 13 și 14 *(notă autor: informarea persoanei vizate*) și orice comunicare și orice măsuri luate în temeiul articolelor 15-22 și 34 (*notă autor: răspunsuri la cererile persoanelor vizate)* sunt oferite gratuit".

Excepția de la regulă este acel caz în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv.

Cine decide caracterul repetitiv al unor astfel de solicitări? Art. 12 alin (5) al GDPR menționează faptul că **operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii**.

Ce poate face operatorul atunci când constată că a primit cereri al căror caracter este unul abuziv, prin repetivitatea lor? Acesta poate:

1. **Fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate.**
2. **Fie să refuze să dea curs cererii.**

Însă, indiferent dacă decide să ceară o taxă ori decide să dea curs cererii, este vital ca operatorul să documenteze procesul prin care a analizat solicitările și a considerat că acestea au un caracter vădit repetitiv și că, prin urmare, sunt nefondate sau excesive.

Cererea trebuie să fie adresată unei anumite persoane din companie sau nu?

Cererile pot fi adresate **oricărei persoane dintr-o organizație**. De aceea, este important ca organizația să-și definească propriile standarde prin intermediul cărora se pot identifica aceste solicitări, se pot direcționa solicitările către persoana responsabilă pentru coordonarea acțiunilor referitoare la protecția datelor personale și se pot furniza răspunsuri, în timp util, persoanelor vizate.

Nu toate organizațiile trebuie să aibă un responsabil cu protecția datelor personale (DPO). Există o serie de criterii care stau la baza definirii cazurilor în care e nevoie de un DPO într-o anumită organizație. Chiar și când nu e nevoie de DPO, însă, în organizația respectivă trebuie să existe o persoană care să fie responsabilă cu coordonarea eforturilor legate de protecția datelor personale.

Existența sau nu a unui DPO nu are legătură cu faptul că acelei companii i se aplică sau nu GDPR. Foarte probabil, aproape tuturor companiilor li se vor aplica prevederile Regulamentului. E greu să existe, spre exemplu, o companie care să nu aibă angajați, să nu aibă clienți ori să nu își vândă într-un fel sau altul, prin campanii de marketing, propriile produse. Prin urmare, întotdeauna e bine să existe cineva în cadrul organizației (DPO sau nu) care să coordoneze activitatea legată de protecția datelor cu caracter personal.

Informarea persoanei vizate

Înainte de orice activitate de prelucrare (există și unele excepții), persoana vizată trebuie informată asupra activității respective. Informarea este obligatorie (e un drept al persoanei vizate) și trebuie să conțină o serie de puncte importante prevăzute în GDPR (art. 13 și 14).

Informarea trebuie realizată indiferent de temeiul utilizat pentru realizarea prelucrării (obligație legală, contract, interes legitim sau consimțământ, ca să le enumerăm pe cele care credem că se potrivesc în acest context).

Informarea trebuie să conțină punctele prezentate mai jos, în funcție de modul în care au fost obținute datele cu caracter personal. Datele sunt obținute, de regulă, direct de la persoana vizată (contract de muncă, CV etc). Există, însă, și situații în care datele sunt obținute indirect (ex. atunci când compania X cumpără compania Y și odată cu această achiziție are acces la baza cu clienți și angajați ai companiei Y).

De asemenea, foarte important este faptul că această informare trebuie realizată de către operator. Cu alte cuvinte, operatorul este cel care răspunde la întrebările de mai jos. Împuternicitul realizează prelucrările Operatorului. Prin urmare, el nu va trebui sa informeze persoana vizată asupra faptului că îi prelucrează datele, pentru că operatorul este cel obligat să o facă. Bineînțeles, operatorul ar trebui să amintească în informare că datele vor fi transferate și către împuterniciții săi în vederea furnizării unor servicii externalizate de contabilitate, salarizare, recrutare personal etc.

Iată un tabel comparativ cu punctele care trebuie incluse într-o informare, atunci când se redactează aceasta[11]:

Ce trebuie să conțină informarea?	**Date obținute direct de la persoana vizată**	**Date obținute indirect de la persoana vizată**
Identitatea și datele de contact ale operatorului (spre exemplu: Denumire companie, Cod fiscal, Adresa poștală, Adresa de email etc.), precum și datele de contact ale responsabilului cu protecția datelor (DPO) din compania în cauză;	✓	✓
Scopul prelucrării datelor, precum și temeiul prelucrării acestora (spre exemplu: prelucrăm email în scopul realizării activității de direct marketing, în baza consimțământului dumneavoastră);	✓	✓

[11] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

Descrierea interesului legitim al operatorului ori al unei terțe părți, acolo unde este aplicabil acest lucru;	✓	✓
Categoriile de date personale prelucrate;		✓
Destinatarii datelor personale, dacă acestea sunt transferate undeva;	✓	✓
Detalii și garanții de securitate adecvate, în cazul în care datele sunt transferate în afara UE;	✓	✓
Perioada de retenție a datelor, ori un criteriu pentru a defini această perioadă de retenție;	✓	✓
Detalierea fiecăruia dintre drepturile pe care le au persoanele vizate;	✓	✓
Dreptul de a-și retrage consimțământul, dacă este aplicabil;	✓	✓
Dreptul de a depune o plângere la Autoritatea de Supraveghere;	✓	✓
Sursa din care sunt colectate datele, precum și menționarea faptului că sursa este una accesibilă public (dacă e cazul);		✓
Dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;	✓	

Existența unui proces decizional automatizat incluzând crearea de profiluri și, cel puțin în acele cazuri, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări.	✓	✓
Când trebuie furnizată informarea?	La momentul la care datele au fost colectate.	Într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună;
		dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă;
		dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară.

Detalierea drepturilor persoanelor vizate

Regulamentul recunoaște persoanelor vizate o serie de 8 drepturi importante (operatorul este cel obligat să se asigure de respectarea lor):

Dreptul la informare

(este detaliat mai sus, la capitolul „Informarea persoanei vizate") - art. 13 și 14 GDPR.

Acesta le permite persoanelor vizate să știe, chiar de la momentul la care se face colectarea (sau în maximum o lună de la dobândirea datelor, în cazul datelor colectate indirect de la persoana vizată) modul în care se vor utiliza acele date, către cine vor fi ele dezvăluite ori transferate, ce drepturi au persoanele în cauză cu privire la datele prelucrate etc.

Dreptul de acces la date

Art. 15 GDPR permite persoanelor vizate să obțină, din partea operatorului, o confirmare că se prelucrează sau nu date cu caracter personal care le privesc și, în caz afirmativ, acces la datele respective și la alte informații utile (art. 15 din GDPR conține o listă a acestor informații utile, printre ele regăsindu-se scopurile prelucrării, categoriile de date prelucrate, destinatarii etc.).

Ca urmare a dreptului de acces, persoana vizată va primi o informare personalizată (vezi conținutul informării, așa cum e prezentat într-un capitol următor), de natură să îi explice ce date îi sunt prelucrate, în ce scop, în ce temei, care e perioada de retenție a acelor date, către cine pot fi ele transferate și în ce scop, menționarea drepturilor pe care le are persoana vizată cu privire la acele drepturi, inclusiv dreptul de a depune o plângere la Autoritatea de Supraveghere, dacă persoana nu e mulțumită de modul în care se redactează acest răspuns etc.

În plus față de această informare cu privire la datele prelucrate, persoana vizată are dreptul de a obține o copie a datelor în cauză. Dacă în cazul informării de mai sus se vorbește despre categorii de date (ex. Adresa de email, nume, etc.), în cazul copiei datelor se vor furniza datele în sine (ion@firma.ro, Ion Popescu etc.).

Dreptul la ștergerea datelor

Art. 17 GDPR permite persoanelor vizate de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate.

Primul lucru pe care ar trebui să îl facă un operator, atunci când primește o astfel de cerere de acces, ar fi să verifice dacă nu cumva se încadrează într-una dintre excepțiile prevăzut de art. 17 alin (3) al GDPR, care îi permite sau îl obligă să păstreze datele, chiar și în ipoteza formulării unei cereri de ștergere.

Cu alte cuvinte, **dreptul la ștergere nu se aplică dacă prelucrarea este necesară**:

(a) pentru exercitarea dreptului la liberă exprimare și la informare;

(b) pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul;

(c) din motive de interes public în domeniul sănătății publice, în conformitate cu articolul 9 alineatul (2) literele (h) și (i) și cu articolul 9 alineatul (3);

(d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în măsura în care dreptul menționat la alineatul (1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau

(e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Exemplu: situația unui angajat care solicită ștergerea datelor sale personale din registrul general de evidență a salariaților. În teorie, admiterea unei astfel de cereri ar pune angajatorul în fața unor sancțiuni drastice din partea autorităților, iar pe salariat l-ar pune în fața unei situații potențiale în care vechimea sa în muncă să fie foarte greu de reconstituit.

La fel, dacă cineva ar solicita ștergerea datelor sale din facturile emise de o companie ori din declarațiile fiscale pe care acea companie le-a depus, acceptarea unei astfel de solicitări ar pune compania în situația de a risca amenzi importante și, poate, alte consecințe în sfera penală.

De aceea, la ambele situații de mai sus, răspunsul clasic pentru o cerere de ștergere va fi de tipul “compania noastră are obligația legală, impusă prin legea / ordinul / etc nr. ../… privind …, să păstreze aceste date, prin urmare nu le vom putea șterge”.

Însă, dacă pe lângă aceste date, compania prelucrează și alte date asupra cărora nu există obligația legală de a le prelucra, iar persoana vizată solicită ștergerea lor, atunci la acea solicitare se va încuviința ștergerea (în măsura în care nu este aplicabilă una din celelalte excepții prevăzute la art. 17 de mai sus).

E posibil ca o companie să prelucreze o dată cu caracter personal (nume, spre exemplu), în cadrul a 4 sau 5 operațiuni de prelucrare. Unele sunt întemeiate pe obligație legală, altele pe contracte, altele pe interes legitim etc. E important de analizat aplicabilitatea excepțiilor de mai sus pe fiecare dintre aceste operațiuni de prelucrare. Dacă se va alege ștergerea pentru datele prelucrate în cadrul uneia dintre operațiunile de prelucrare, acest lucru nu va afecta prelucrarea datelor în cauză pe alte operațiuni. Prin urmare, e important ca prelucrările sa fie concepute, astfel încât ștergerea datelor pe o operațiune să nu afecteze alte operațiuni.

Dreptul la rectificarea datelor

Conform Art. 16 GDPR: persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea sau completarea datelor cu caracter personal inexacte care o privesc.

Exemplu: Un operator de date personale ar trebui să implementeze un sistem care să asigure rectificarea și completarea datelor prelucrate, în măsura în care aceasta este posibilă (ex. dacă un salariat dorește să-și schimbe numele de familie, trebuie să poată prezenta o hotărâre judecătorească ori administrativă care atestă această schimbare, pentru ca ea să poată fi operată în actele companiei) sau în măsura în care aceasta este utilă (ex. un salariat dorește să se menționeze în dosarul său de personal faptul că a fost căsatorit de n ori, fapt care nu ajută deloc dosarul de personal și ar putea constitui o prelucrare excesivă de date).

Dreptul la restricționarea datelor

Art. 18 GDPR: dreptul la restricționarea datelor este un drept cu caracter temporar. În unele situații, între momentul în care, spre exemplu, operatorul ia decizia de a șterge anumite date (nu mai are nevoie de datele cu caracter personal în scopul prelucrării) și ștergerea efectivă a datelor, persoana vizată face o cerere prin care se opune ștergerii, motivând faptul că i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță. Ca urmare a unei astfel de solicitări, operatorul "îngheață" datele oprind prelucrarea lor pentru o anumită perioadă de timp.

Aceasta "înghețare" poate însemna marcarea datelor în sistem, pentru a nu mai fi prelucrate până se ia decizia în privința lor, mutarea datelor în alt sistem până se ia o decizie etc.

În toate cazurile, însă, la momentul ridicării restricției de prelucrare, Operatorul trebuie să informeze persoana vizată cu privire la faptul ca s-a ridicat restricția.

Dreptul la portabilitatea datelor

Art. 20 GDPR. Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-

au fost furnizate datele cu caracter personal. Cu alte cuvinte, datele personale trebuie să poată fi oferite persoanei vizate, într-un format structurat, pentru ca această să poată decide că le descarcă sau, dimpotrivă, că le poate trimite unui alt operator.

Acest drept se aplica doar în măsura în care datele sunt prelucrate în temeiul unui contract sau al consimțământului persoanei vizate, precum și (cumulat) atunci când prelucrarea se face prin mijloaceautomate.

Dreptul la portabilitatea datelor se aplică atât asupra datelor furnizate direct de persoana vizată, cât și asupra datelor observate de operator (cele pe care operatorul le observă cu privire la persoana vizată, colectându-le, astfel, direct de la persoana în sine, dar ca aceasta să le furnizeze). Sunt excluse de la portabilitate datele derivate sau deduse, așa cum sunt denumite, de regulă, concluziile pe care le trag operatorii (pe baza unor operațiuni de profilare, de regulă) cu privire la persoanele vizate.

Dreptul la opoziție

Art. 21 GDPR. Persoana vizată are dreptul de a se opune, spre exemplu, prelucrării datelor sale personale, atunci când acestea sunt prelucrate în scop de marketing direct. E foarte important ca, atunci când există prelucrări care ar putea da naștere acestui drept pentru persoana vizată, în informare să fie menționată existența acestui drept.

Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată

Atunci când se întâmplă o operațiune de profilare, efectele ei pot fi de mai multe tipuri.

E posibil ca profilarea să nu fie urmată de o decizie automatizată (spre exemplu, în cazul unui credit, profilarea e toată operațiunea de strângere de date prin care Banca observă în ce măsură solicitantul se încadrează în standardele ei de creditare, dar decizia de acordare a creditului e luată de o persoană fizică).

În acest caz, persoana vizată are dreptul de a se opune unei astfel de prelucrări și va trebui informată înainte de realizarea acestui tip de prelucrare (inclusiv cu date referitoare la logica minimă utilizată și consecințele pe care le are utilizarea acelor decizii automatizate). Ea poate solicita intervenția umană în procesul respectiv și poate contesta procesul printr-o plângere la Autoritate.

Cum se construiește relația cu partenerii de afaceri?

Contractul operator - împuternicit

Între operator și împuternicit trebuie să existe un contract. E foarte important ca **acest contract să fie documentat (să poată fi probat)**, prin urmare este esențială existența unui **contract scris** (nu neapărat pe hârtie, chiar și în formă electronică, dar respectând condițiile de validitate ale contractului).

Acest contract (denumit Acord de Prelucrare a Datelor cu Caracter Personal) poate fi, foarte bine, o anexă la contractele existente sau contractele noi.

Contractul ajută ambele părți să își definească atât sarcinile, cât și responsabilitățile pe care le presupune relația lor. Mai mult, pentru împuternicit, contractul este actul care punctează instrucțiunile precise pe care le transmite operatorul și care definește, astfel, rolul și responsabilitățile fiecăreia dintre părți.

Împuternicitul răspunde (poate fi sancționat de Autoritatea de Supraveghere, ori acționat în judecată de către persoana vizată) în două situații: când nu respectă instrucțiunile transmise de operator, respectiv când nu respectă obligațiile impuse lui, punctual, de către GDPR.

Atenție! Este, însă, de reamintit poziția consultantului în astfel de relatii comerciale, pentru că nu întotdeauna, pe anumite tipuri de operațiuni, suntem într-o relație de tipul operator – împuternicit. Dacă vorbim despre o relație operator – operator, atunci regulile de mai sus nu sunt aplicabile, pentru ca articolul 28 din GDPR se referă, specific, la reglementarea situației în care un operator împuternicește pe cineva să realizeze o anumită operațiune de prelucrare pentru el.

Cum spuneam, în multe situații, poziția consultantului nu e neapărat una de împuternicit, pe anumite părți ale prelucrarii sale. Potrivit Autorității de Supraveghere din Marea Britanie[12],

> În aceste cazuri, clientul nu va avea responsabilitatea exclusivă a operatorului de date, chiar dacă a inițiat colaborarea, solicitând sfaturi sau comandând un raport. Responsabilitatea revine și furnizorului de servicii profesionale în sine, deoarece acesta determină ce informații trebuie obținute și prelucrate pentru a face munca și pentru că este furnizorul este răspunzător pentru conținutul muncii sale.
>
> Utilizarea unui avocat oferă o bună ilustrare a motivului pentru care furnizorii de servicii profesionale nu sunt, de obicei, doar împuterniciți. Un client primește consultanță juridică și, indiferent dacă alege sau nu să urmeze sfatul, nu ar cere avocatului să modifice recomandările originale - avocatul controlează conținutul detaliat al sfaturilor. Avocații ar avea de asemenea propriile responsabilități profesionale în ceea ce privește păstrarea evidenței, confidențialitatea comunicațiilor și așa mai departe. Din nou, aceasta indică faptul că avocații și furnizorii de servicii profesionale similare sunt operatori în nume propriu.

Este, deci, vital să calificăm relația cu partenerii de afaceri nu per ansamblu, ci pe tipuri de operațiuni de prelucrare. O entitate nu poate fi și operator și împuternicit pentru aceeași operațiune de prelucrare. Poate fi ori una, ori cealaltă. Pe operațiuni de prelucrare diferite, însă, poate avea roluri diferite.

Situația contractului de mai jos, deci, vizează operațiunile pentru care vorbim despre o relație de tipul operator – împuternicit între client și consultant, nu despre situațiile în care vorbim despre

[12] https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

o relație de tipul operator – operator, când părțile nu-și pot da instrucțiuni una celeilalte (clientul nu poate da instrucțiuni consultantului, atunci când vorbim despre obligații profesionale raportate la actele normative referitoare la prevenirea şi sancţionarea spălării banilor, spre exemplu).

Situații minime pe care trebuie sa le cuprindă contractul de prelucrare a datelor cu caracter personal

Noutatea pe care o impune GDPR constă în faptul că obligă părțile să includă în contract o serie de prevederi importante:

1. obiectul și durata prelucrării,
2. natura și scopul prelucrării,
3. tipul de date cu caracter personal,
4. categoriile de persoane vizate,
5. obligațiile și drepturile operatorului.

În plus, GDPR impune ca, în contractul încheiat între părți, împuternicitul să se asigure, printre altele de următoarele:

1. **Trebuie să acționeze numai pe baza instrucțiunilor scrise ale operatorului (cu excepția cazului în care legea solicită să acționeze fără astfel de instrucțiuni).**

   Instrucțiunile operatorului sunt, de fapt, acele explicații și solicitări care îl ajută pe împuternicit să știe în orice moment ce are de făcut, fără să fie nevoie să ia el decizii în această privință. Orice companie în calitate de Împuternicit nu ar trebui să ia niciun fel de decizie cu privire la prelucrările pe care le face în numele operatorului. În această calitate trebuie ca, atunci când este în dubiu cu privire la un anumit lucru, să întrebe operatorul și să îi solicite acestuia instrucțiuni detaliate cu privire la modul în care se va realiza respectiva prelucrare.

   Atunci când împuternicitul nu respectă aceste obligații și ia el însuși decizii cu privire la prelucrare, poate să se pună în poziția operatorului și va putea fi făcut răspunzător pentru problemele generate de acea prelucrare. De aceea, existența inițială a unui set de instrucțiuni cu privire la datele care trebuie prelucrate și modalitățile în care se va realiza prelucrarea acelor date este vitală pentru cazurile când compania are calitatea de împuternicit.

2. **Trebuie să se asigure că persoanele care prelucrează datele sunt supuse unei obligații de confidențialitate.**

   Cu alte cuvinte, în contractele de muncă sau în contractele de colaborare cu acestea, vor trebui inserate clauze de confidențialitate care să asigure Împuternicitul și Operatorul de faptul că acele persoane sunt instruite și știu cum să pastreze secretul asupra datelor la care au acces.

3. **Trebuie să ia măsurile adecvate pentru a asigura securitatea prelucrării (aderarea la un cod de conduită al industriei ori aderarea la un mecanism de certificare pot fi utilizate ca elemente prin care să se demonstreze existența garanțiilor suficiente).**

   În acest moment, în multe industrii se redactează coduri de conduită utile pentru respectarea,

de către împuterniciți, a acestei obligații. Dincolo de aceste coduri de conduită, însă, împuternicitul va trebui să ia măsuri tehnice, menționate în capitolele anterioare, pentru a asigura operatorul că nu există riscuri cu privire la datele personale pe care le prelucrează în numele acestuia.

De asemenea, Împuternicitul va trebui să îi poată oferi Operatorului, dacă e nevoie, un audit asupra capabilităților sale tehnice și organizatorice de natura să asigure securitatea prelucrărilor, dacă operatorul îi cere acest lucru.

4. **Nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului.**

   Una dintre regulile principale care vor trebui detaliate în contract este situația sub-împuterniciților. Exemplu: dacă Compania X externalizează serviciul HR ori serviciul de contabilitate către Compania Y, în ce condiții va putea compania Y să sub-contracteze acest serviciu, în tot sau în parte, către o altă companie? Va trebui Compania Y să ceară de fiecare dată acordul Companiei X cu privire la partenerul către care se va subcontracta serviciul inițial? Sau va fi aplicabil un acord general care spune că, atâta vreme cât Compania Y informează compania X cu privire la identitatea partenerului către care a subcontractat, atunci totul este în regulă?

   Subcontractarea ar putea viza doar părți tehnice ale infrastructurii de gestionare a serviciului de contabilitate (ex. Serviciul de cloud al unui furnizor de software conta). E important, deci, de lămurit această situație, înainte ca în contract să se prevadă lucruri ce vor îngreuna, ulterior, serios, modul în care se realizează furnizarea serviciului.

5. **Trebuie să asiste operatorul de date în asigurarea accesului la subiect și să permită persoanelor vizate să își exercite drepturile în temeiul GDPR.**

   Este obligația operatorului să răspundă la cererile persoanelor vizate. Singura obligație pe care o are împuternicitul este aceea de a prelua cererile (dacă ajung la el și sunt țintite spre operator) și de a le trimite mai departe către operator.

   Împuternicitul nu răspunde la acele cereri, iar acest lucru e explicabil relativ simplu: împuternicitul poate fi una dintre cele x verigi ale lanțului de prelucrare pe care îl realizează un operator. Dacă împuternicitul ar răspunde, ar face-o doar cu privire la datele care se află în sistemele sale. Or, în realitate, operatorul ar putea prelucra datele persoanei vizate în cauză în mult mai multe sisteme, proprii sau aparținând altor împuterniciți.

   Prin urmare, dacă împuternicitul ar răspunde, i-ar oferi persoanei vizate doar o frântură din informațiile pe care și le dorește. Împuternicitul nu va face altceva decât să își respecte condiția de “vas comunicant” și să preia cererile de la persoanele vizate, atunci când acestea ajung la el, să le transmită operatorului, respectiv să preia răspunsul operatorului și să îl transmită persoanei vizate (atunci când împuternicitul este unicul punct de contact cu persoana vizată).

6. **Trebuie să asiste operatorul de date în îndeplinirea obligațiilor sale privind GDPR în ceea ce privește securitatea prelucrării, notificarea privind incidentele de securitate și evaluările de impact ale protecției datelor.**

7. **Trebuie să șteargă sau să returneze toate datele personale către operator, după cum este solicitat la încetarea contractului;**

8. **Trebuie să permită desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea**, să furnizeze auditorilor toate informațiile necesare pentru a se asigura că ambele părți îndeplinesc obligațiile prevăzute la articolul 28 și să informeze imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă prezentul regulament sau alte dispoziții din dreptul intern sau din dreptul Uniunii referitoare la protecția datelor;

9. **Trebuie să coopereze cu Autoritatea de Supraveghere**, potrivit art. 58 al GDPR;

10. **Trebuie să numească un DPO**, dacă acest lucru este necesar;

11. **Trebuie să țină evidența activităților de prelucrare**;

12. **Trebuie să numească (în scris) un reprezentant în cadrul Uniunii Europene**, dacă este necesar.

În momentul în care alege să transmită o parte din obligațiile sale unor alți împuterniciți, împuternicitul trebuie să transmită, în cascadă, instrucțiunile și obligațiile primite de la operator. Mai mult, conform art. 28 alin (4) al GDPR, transmiterea trebuie să vizeze în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentului regulament.

În cazul în care această a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor, persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor acestei a doua persoane împuternicite.

Riscul, în relația dintre operator și împuternicit

Punctul esențial al relației dintre operator sau împuternicit este definit în articolul 28 alin (10) al Regulamentului, care menționează **riscul cel mai important la care se expune împuternicitul atunci când alege să facă mai mult decât a fost instructat**.

În cazul în care o persoană împuternicită de operator încalcă prezentul regulament, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă, asumându-și astfel atât rolul, cât și răspunderea pentru această poziție.

Acord de Prelucrare a Datelor cu Caracter Personal nu este un contract comercial, semnat între părți. Acolo, părțile negociază preț, livrabile și alte obligații specifice, date de fiecare produs ori serviciu în parte. Acest Acord, menționat și impus de GDPR, este cel care **privește operațiunile de prelucrare de date cu caracter personal pe care le presupune colaborarea dintre cele două părți**. El poate fi întocmit ca un contract separat ori un capitol în contractul comercial dintre cele două părți ori o anexă la acest contract.

Mai mult, dacă împuternicitul nu regăsește în negocierile inițiale și contractul semnat inițial o serie de instrucțiuni legate de un tip nou de prelucrare pe care o va face în numele operatorului, părțile trebuie să rezolve acest aspect prin emiterea unui set suplimentar de instrucțiuni pe care împuternicitul să le urmeze.

Când răspunde împuternicitul pentru acțiunile sale

Împuternicitul poate fi responsabil pentru plata unor despăgubiri oricărei persoane care suferit un prejudiciu material sau moral ca urmare a unei încălcări aîn situații precum următoarele:

1. **când depășește limitele ori ignoră instrucțiunile transmise de către operator**, intrând astfel sub incidența articolului 28 alin (10) al GDPR[13] despre care menționam mai sus (în cazul în care o persoană împuternicită de operator încălcă prezentul regulament, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă);

2. **când nu respectă obligațiile impuse lui de către GDPR** (vezi mai sus). E foarte importantă existența contractului scris și documentabil între cele două părți. Menționarea cât mai amănunțită a instrucțiunilor este vitală pentru împuternicit, pentru că acele instrucțiuni sunt singura lui dovadă că a acționat în interiorul lor, atunci când se va pune problema angajării răspunderii sale pentru diverse tipuri de operațiuni de prelucrare realizate în numele operatorului.

În privința amenzilor impuse de Autoritatea de Supraveghere, atunci când se ia decizia dacă să se impună o amendă administrativă și decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenția cuvenită următoarelor aspecte (acestea sunt valabile și în cazul amenzilor impuse operatorului, nu doar împuternicitului):

A. **natura, gravitatea și durata încălcării**, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;

B. dacă încălcarea a fost **comisă intenționat sau din neglijență**;

C. orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a **reduce prejudiciul suferit de persoana vizată**;

D. gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ținându-se seama de **măsurile tehnice și organizatorice implementate** de aceștia în temeiul articolelor 25 și 32;

E. **eventualele încălcări anterioare relevante** comise de operator sau de persoana împuternicită de operator;

F. gradul de cooperare cu Autoritatea de Supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării;

G. **categoriile de date cu caracter personal afectate de încălcare**;

H. **modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere**, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;

[13] Art. 28 alin (10), GDPR: ”în cazul în care o persoană împuternicită de operator încălcă prezentul regulament, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă”.

I. în cazul în care măsurile menționate la articolul 58 alineatul (2) au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la același obiect, **respectarea respectivelor măsuri**;

J. **aderarea la coduri de conduită aprobate**, în conformitate cu articolul 40, sau la mecanisme de certificare aprobate, în conformitate cu articolul 42; și

K. **orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului**, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

Ce clauze ar trebui să cuprindă un contract de prelucrare a datelor cu caracter personal?

Iată o trecere în revistă a unor clauze extrem de importante, care ar trebui menționate în contractele de prelucrare a datelor cu caracter personal pe care le încheie operatorul și împuternicitul.

Contractul ar trebui să menționeze, pentru început:

- operațiunea de prelucrare vizată si durata prelucrării;
- natura și scopul prelucrării;
- categoriile de date personale care vor fi implicate și tipurile de persoane vizate implicate; și
- drepturile și obligațiile operatorului.

Contractul va trebui să includă, de asemenea, un minim al clauzelor următoare, solicitând împuternicitului să:

- acționeze doar pe baza instrucțiunilor specifice ale operatorului;
- se asigure că oamenii care prelucrează datele au inserate în contractele lor de muncă prevederi specifice privind clauze de confidențialitate;
- ia măsuri necesare pentru a asigura securitatea prelucrării;
- nu recruteze o altă persoană împuternicită (să nu subcontracteze) fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecții față de aceste modificări;
- transmită mai departe, în cazul în care recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator;
- rămână pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor sub-contractorilor, în cazul în care această a doua persoană împuternicită (sub-contractorul) nu își respectă obligațiile privind protecția datelor;
- asiste operatorul în rezolvarea cererilor persoanelor vizate și să le permită persoanelor vizate să-și exercite drepturile recunoscute de GDPR;
- asiste operatorul în indeplinirea obligațiilor sale referitoare la securitatea prelucrărilor, notificarea incidentelor de securitate și realizarea evaluărilor de impact asupra protecției datelor;
- șteargă ori să returneze datele personale către Operator, la cererea acestuia, la momentul încetării contractului; și să

- pună la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la prezentul articol,
- permită desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat (și contribuie la acestea)
- informeze imediat operatorul în cazul în care, în opinia sa, o instrucțiune GDPR sau alte dispoziții din dreptul intern sau din dreptul Uniunii referitoare la protecția datelor.

Autoritățile de Supraveghere pot alege să adopte clauze contractuale standard pentru aspectele menționate mai sus.

Securitatea datelor personale și consecințele incidentelor de securitate

GDPR impune atât operatorului, cât și împuternicitului, obligația de a lua măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător riscului cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice.

Regulamentul nu impune o listă de măsuri de securitate (nici n-ar fi posibil acest lucru), ci amintește o serie de acțiuni care ar putea intra în această categorie:

1. pseudonimizarea (înlocuirea cu un pseudonim- ca o măsură de securitate) și criptarea datelor cu caracter personal;
2. capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă a sistemelor și serviciilor de prelucrare;
3. capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care există un incident de natură fizică sau tehnică;
4. un proces de încercare, evaluare și apreciere periodică a eficacității măsurilor tehnice și organizatorice pentru garantarea securității prelucrării;
5. aderarea la un cod de conduită aprobat, menționat la articolul 40;
6. aderarea la un mecanism de certificare aprobat, menționat la articolul 42;

O atenție deosebită trebuie să se acorde așa numitelor „incidente de securitate” (traduse în versiunea în limba română a Regulamentului ca fiind încălcări ale securității datelor cu caracter personal).

Potrivit regulamentului, „încălcarea securității datelor cu caracter personal” înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la:

- **distrugerea,**
- **pierderea,**
- **modificarea,**
- **divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod sau la**
- **accesul neautorizat la acestea.**

Ori de câte ori are loc un incident de securitate, operatorul trebuie să analizeze incidentul și să decidă câteva lucruri importante:

1. **Care este data la care a luat cunoștință de acel incident de securitate?** De regulă, indicii pot exista mai devreme, dar certitudinea că suntem în prezența unui incident de securitate și nu în prezența unei probleme tehnice sau organizatorice de altă natură se întâmplă doar după ce se anchetează acele indicii și se ia o decizie pe baza informațiilor aflate în ancheta respectivă.

   Este foarte important să se fixeze în timp momentul la care s-a aflat despre un astfel de incident de securitate, pentru că de acel moment vor depinde câteva acțiuni ulterioare. De asemenea, alături de fixarea momentului, trebuie documentate și alte aspecte legate de respectivul incident, cum ar fi numărul persoanelor vizate afectate, tipul de categorii de date cu caracter personal

afectate, consecințele prevăzute ale incidentului respectiv pentru persoanele vizate, modul în care se pot limita sau înlătura aceste consecințe.

2. Dacă s-a documentat existența unui incident de securitate, **operatorul va trebui să analizeze riscurile pe care le implică acel incident pentru drepturile și libertățile persoanelor vizate**. Exemplu: un operator care stochează cărți de debit, alături de codul CVV, dacă o altă persoană a avut acces la acele numere de cărți de debit, fără autorizare, ar putea presupune, pentru persoanele vizate, riscul ca banii din conturile lor să dispară oricând. Prin urmare, vorbim despre un risc evident.

3. Dacă **există** un astfel de **risc**, atunci va trebui notificată Autoritatea de Supraveghere.

   Atenție, în traducerea oficială a Regulamentului, în limba română, la art. 33 alin (1) s-a strecurat o eroare importantă. Notificarea Autorității se face, cum spuneam, **la momentul la care există un risc**. Regulamentul prevede, ca idee, această obligație într-o topică mai ciudată: "notificarea se face întotdeauna, cu excepția cazului în care nu există un risc...". în traducerea în limba română, această topică a fost enunțată uitându-se cuvântul "nu", astfel încât ea a devenit "notificarea se face întotdeauna, cu excepția cazului în care există un risc" (lipsește, deci, acel „nu", care face diferența). Chiar dacă, foarte probabil, va apărea o corectură oficială a traducerii, o sugestie importantă e că, ori de câte ori e nevoie de consultarea GDPR, să vă raportați la varianta în limba engleză.

   Notificarea Autorității de Supraveghere va cuprinde:

   - identitatea organizației care face notificarea;
   - numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
   - descrierea caracterului incidentului ("ce s-a întâmplat concret", adică);
   - acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză;
   - acolo unde este posibil, categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
   - descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
   - măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

4. Dacă riscul identificat este unul **ridicat**, atunci operatorul va fi obligat să informeze și persoana vizată cu privire la acel incident de securitate.

   Notificarea persoanelor vizate va cuprinde:

   - numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
   - descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
   - măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Care este rolul împuternicitului în cazul incidentelor de securitate?

Mai e important de menționat faptul că **obligația împuternicitului este să informeze întotdeauna operatorul cu privire la apariția unor indicii de producere a unor incidente de securitate**. În măsura în care aceste incidente se întâmplă, e important de menționat faptul că **operatorul este singurul în măsură să analizeze atât existența lor, cât și gradul de risc** pe care îl presupun incidentele în cauză.

Rolul împuternicitului este acela de a asista operatorul în această analiză, precum și de a-l asista în depunerea notificării către autoritate, respectiv în investigația următoare care ar putea apărea de la Autoritate, cu privire la incident.

Birocrația GDPR

Registrul operațiunilor de prelucrare

GDPR impune atât operatorului, cât și împuternicitului obligația de a documenta pașii pe care îi fac atunci când prelucrează date cu caracter personal. O parte a acestei acțiuni de documentare este reprezentată de existența în formă scrisă (inclusiv electronic) a unui "registru al operațiunilor de prelucrare".

Registrul operațiunilor de prelucrare se regăsește la art. 30 al Regulamentului și e obligatoriu pentru (aproape) toate organizațiile care prelucrează date personale, indiferent dacă sunt împuterniciți sau operatori.

Există o discuție în media românească, privind faptul că GDPR permite companiilor sub 250 de angajați să nu realizeze Registrul Operațiunilor de Prelucrare. În realitate, sunt puține companiile care se pot folosi de această excepție, din moment ce ea se aplica doar atunci:

- când prelucrarea este ocazională,
- când prelucrarea pe care o efectuează nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate,
- când prelucrarea nu include categorii speciale de date,
- când prelucrarea nu include date cu caracter personal referitoare la condamnări penale și infracțiuni.

După cum se observă, e greu de crezut că putem vorbi despre o organizație care să prelucreze date personale doar în mod ocazional (orice organizație are măcar angajați sau clienți, dacă nu și alte categorii de persoane vizate cărora le prelucrează datele în mod sistematic și nu ocazional).

Ce conține registrul operațiunilor de prelucrare, atunci când el este realizat de către operator? Art. 30 alin (1) din Regulament menționează toate aspectele care trebuie incluse:

1. numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
2. scopurile prelucrării;
3. o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
4. categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
5. dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la articolul 49 alineatul (1) al doilea paragraf, documentația care dovedește existența unor garanții adecvate;
6. acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
7. acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).

Dup[cum vedeți, în registrul operațiunilor de prelucrare se completează multe dintre răspunsurile pe care le-am dat în setul de întrebări pe care le-am urmat în procesul de proiectare a unei operațiuni de prelucrare de la începutul acestui document.

Atunci când registrul este realizat de către împuternicit, pentru operațiunile de prelucrare realizate în numele operatorului (dacă un împuternicit lucrează cu mai mulți operatori, trebuie să realizeze un astfel de registru pentru fiecare operator în numele căruia lucrează):

1. numele și datele de contact ale fiecărui operator în numele căruia acționează, precum și ale reprezentantului operatorului sau numele și datele de contact al persoanei împuternicite de operator, după caz;

2. categoriile de activități de prelucrare desfășurate în numele fiecărui operator;

3. dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor prevăzute la articolul 49 alineatul (1) al doilea paragraf din Regulament, documentația care dovedește existența unor garanții adecvate;

4. acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1) din Regulament.

Registrul e foarte important și în relația cu Autoritatea de Supraveghere. Ori de câte ori Autoritatea solicită operatorului sau împuternicitului acest Registru, el trebuie pus la dispoziția Autorității.

Modele de registre se pot consulta online pe siteul Autorităților de Supraveghere din Franța[14] și Marea Britanie[15].

Responsabilul cu protecția datelor cu caracter personal (DPO)

Unele organizații vor trebui să-și numească un responsabil cu protecția datelor cu caracter personal. E importantă mențiunea, reluată și mai sus în acest manual, că numirea unui responsabil nu este echivalentă cu aplicarea GDPR asupra organizației în sine. GDPR este, foarte probabil, aplicabil chiar dacă organizația nu îndeplinește acele condiții necesare pentru a avea un DPO. Aplicarea GDPR unei organizații nu are legătură cu GDPR-ul, ci cu faptul că organizația în sine prelucrează date cu caracter personal altfel decât ocazional.

Sunt obligate să își numească un responsabil:

1. instituțiile publice (cu excepția instanțelor de judecată),

2. companiile a căror activitate principală constă în operațiuni de prelucrare care necesită o monitorizare periodică și sistematică pe scară largă a persoanelor vizate, **(notă: trebuie îndeplinite cumulativ toate aceste condiții pentru a fi nevoie de un DPO).**

3. companiile a căror activitate principală constă în operațiuni de prelucrare, pe scară largă, a unor categorii speciale de date (originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice, apartenența la sindicate, date genetice, date biometrice, date privind sănătatea, date privind viața sexuală sau orientarea sexuală) sau date referitoare la condamnări

[14] https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx
[15] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities

penale și infracțiuni **(notă: trebuie îndeplinite cumulativ toate aceste condiții pentru a fi nevoie de un DPO).**

Cel mai important document la care trebuie să vă raportați atunci când veți analiza nevoia unui DPO în organizația dvs. este, dincolo de prevederile GDPR, Ghidul privind Responsabilul cu protecția datelor ('DPOs'), emis de Grupul de Lucru Art. 29, la 5 aprilie 2017.

Cel mai important criteriu, de ținut minte atunci când vorbim despre numirea unui DPO, este ideea "activității principale". În această privință, Ghidul oferă explicații utile[16].

> De exemplu, activitatea principală a unui spital este de a oferi asistență medicală. Cu toate acestea, un spital nu poate oferi asistență medicală în condiții de siguranță și în mod eficient fără prelucrarea datelor privind starea de sănătate, cum ar fi dosarele medicale ale pacienților. Prin urmare, prelucrarea acestor date ar trebui să fie considerată a fi una dintre activitățile principale în orice spital și, prin urmare, spitalele trebuie să desemneze un DPO.
>
> Ca un alt exemplu, o companie de securitate privată efectuează supravegherea unui număr de centre comerciale private și spații publice. Supravegherea este activitatea de bază a companiei, care, la rândul său, este indisolubil legată de prelucrarea datelor cu caracter personal. Prin urmare, această societate trebuie să desemneze, de asemenea, un DPO.
>
> Pe de altă parte, toate organizațiile efectuează anumite activități, spre exemplu, plata angajaților lor sau deținerea de activități standard de suport IT. Acestea sunt exemple de funcții de sprijin necesare pentru activitatea de bază sau principală a organizației. Chiar dacă aceste activități sunt necesare sau esențiale, acestea sunt de obicei considerate mai degrabă funcții auxiliare decât activitate principală.

În privința criteriului "prelucrării pe scară largă", se recomandă ca următorii factori să fie luați în considerare atunci când se stabilește dacă prelucarea este efectuată pe o scară largă:

- numărul persoanelor vizate – ori un număr exact ori un procent din populația relevantă;
- volumul datelor și/sau gama de elemente diferite de date în curs de prelucrare;
- durata sau permanența activității de prelucrare a datelor;
- suprafața geografică a activității de prelucrare.

Exemple de prelucrări pe scară largă includ:

- prelucrarea datelor pacienților în activitatea regulată a unui spital;
- prelucrarea datelor de călătorie a unei persoane fizice ce utilizează sistemul de transport public (spre exemplu, urmărire cu ajutorul cardurilor de călătorie);
- prelucrarea în timp real a datelor de geolocalizare a clienților unei rețele internaționale de fast-food în scopuri statistice de către o persoană împuternicită de operator specializată în furnizarea serviciilor de acest tip;
- prelucrarea datelor clienților în activitatea regulată a unei companii de asigurări sau a unei bănci;
- prelucrarea datelor personale de către un motor de căutare în scop de publicitate comportamentală;
- prelucrarea datelor (conținut, trafic, localizare) de către furnizorii de telefonie sau servicii de Internet.

[16] http://www.dataprotection.ro/servlet/ViewDocument?id=1384

Ghidul vorbește despre faptul că nu constituie o prelucrare pe scară largă prelucrarea datelor pacientului de către un medic individual. Mai mult, potrivit preambulului nr. 91 al GDPR, ”prelucrarea datelor cu caracter personal nu ar trebui considerată a fi la scară largă în cazul în care prelucrarea se referă la date cu caracter personal de la pacienți sau clienți de către un anumit medic, un alt profesionist în domeniul sănătății sau un avocat”. **E plauzibilă, deci, concluzia că, și în cazul activității unui contabil individual, nu există necesitatea numirii unui DPO**. Însă, chiar e important ca această situație să fie analizată în funcție de cazul dumneavoastră particular.

Cât privește celelalte criterii, monitorizarea comportamentului persoanelor vizate, spre exemplu, include toate formele de urmărire și de creare de profiluri pe internet, inclusiv în scopuri de publicitate comportamentală, dar nu trebuie limitată doar la mediul online. Trebuie analizat în ce măsură activitatea companiei dumneavoastră îndeplinește această condiție a monitorizării persoanelor vizate, pentru că, în multe cazuri, nu putem vorbi despre o monitorizare așa cum o definește GDPR.

Potrivit, indicațiilor[17] Autorității Naționale privind Supravegherea Prelucrării Datelor cu Caracter personal, exemple de situații care pot constitui o monitorizare periodică și sistematică a persoanelor vizate:

- gestionarea unei rețele de telecomunicații;
- profilare și scoring în scopul evaluării riscurilor (de exemplu, în scopul acordării unui credit, stabilirea primelor de asigurare, de prevenire a fraudelor, detectarea spălării banilor);
- urmărirea locației, spre exemplu prin aplicații mobile (geolocalizare);
- desfășurarea de programe de loialitate;
- monitorizarea stării de sănătate prin intermediul dispozitivelor portabile;
- televiziune cu circuit închis - CCTV;
- prelucrarea datelor pacienților de către un spital;
- prelucrarea datelor datelor de conținut, locație, trafic de către furnizorii de servicii de internet;
- prelucrarea datelor personale de către companii de asigurări;
- publicitate comportamentală.

Tot Ghidul Grupului de Lucru Art. 29 menționează că ”este important să se sublinieze faptul că, chiar dacă operatorul îndeplinește criteriile de desemnare obligatorie, persoana împuternicită de respectivul operatorul nu trebuie neapărat să numească un DPO. Totuși, acest lucru poate reprezenta o bună practică”.

Exemplul menționat în ghid este extrem de util în această situație:

> O mică afacere de familie activă în distribuția de aparate de uz casnic într-un singur oraș folosește serviciile unei persoanei împuternicite de operator a cărui activitate de bază este de a oferi servicii de asistență și analiză pe pagina web cu activități specifice de publicitate și marketing. Activitățile afacerii de familie și clienții săi nu generează prelucrarea datelor pe „scară largă”, având în vedere numărul mic de clienți și activitățile relativ limitate. Cu toate acestea, activitățile persoanei împuternicite de operator, având mulți clienți precum această mică întreprindere, luate împreună, efectuează prelucrări de date pe scară largă. Prin urmare, persoana împuternicită de operator trebuie să desemneze un DPO în temeiul art. 37(1)b). În același timp, afacerea de familie în sine nu are obligația de a desemna un DPO.

Ce pregătire ar trebui să aibă un DPO?

[17] http://www.dataprotection.ro/?page=Responsabilul_cu_protectia_datelor&lang=ro

Potrivit GDPR, un DPO „este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile în domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la art. 39". Preambulul 97 al GDPR prevede că nivelul necesar al cunoștințelor de specialitate ar trebuie să fie stabilit în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate.

Cu alte cuvinte, nu este necesară, cel puțin la data redactării acestui material, o certificare pe baza căreia să fie numit un astfel de DPO în cadrul unei organizații. El trebuie să aiba cunoștințe privind legislația de protecție a datelor, precum și cunoștințe tehnice privind activitatea care se desfășoară. E greu de crezut că, altfel decât forțând lucrurile, ar putea există un organism care să pregatească DPO pentru activitățile tehnice extrem de variate din lumea reală.

Funcția de DPO a fost introdusă în COR, prin intermediul Ordinului Ministerului Muncii nr. 1.786/2017, sub forma responsabil cu protecția datelor cu caracter personal (242231).

Ce anume face un DPO în cadrul unei organizații?

Simplist vorbind, art. 38 din GDPR impune organizației ca DPO să fie „implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal". Cu alte cuvinte, în cuvintele Ghidului Grupului de Lucru:

- DPO este invitat să participe în mod regulat la ședințele conducerii la nivel înalt și la nivel mediu.
- Prezența DPO este recomandată în cazul în care se iau decizii cu implicații asupra protecției datelor. Toate informațiile relevante trebuie să fie transmise DPO în timp util pentru a permite ca acesta să ofere o consiliere corespunzătoare.
- Avizului DPO trebuie să i se acorde întotdeauna o importanță deosebită. În caz de dezacord, Grupul de Lucru recomandă, ca bună practică, documentarea motivelor pentru care nu a fost urmat avizul DPO.
- DPO trebuie să fie consultat cu promptitudine imediat ce a avut loc o încălcare a securității datelor sau un alt incident.
- Atunci când este cazul, operatorul sau persoana împuternicită de operator ar putea elabora ghiduri privind protecția datelor sau proceduri care stabilesc situații când DPO trebuie să fie consultat.

Merită menționate, de asemenea, alte lucruri în privința activității unui DPO:

- "asigurarea resurselor necesare pentru exercitarea sarcinilor sale, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate" (art. 38 alin 2 GDPR);
- operatorii/persoanele împuternicite de operator trebuie să se asigure că DPO „nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea sarcinilor sale". Considerentul 97 adaugă faptul că DPO „indiferent dacă este sau nu angajat al operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent". (art. 38 alin 3 GDPR;
- DPO nu poate „să fie demis sau sancționat de operator sau persoana împuternicită de operator pentru îndeplinirea sarcinilor sale" (art. 38 alin 3 GDPR);
- DPO poate „să îndeplinească și alte sarcini și atribuții", dar organizația trebuie să se asigure că „niciuna dintre aceste sarcini și atribuții nu generează un conflict" (art. 38 alin 6 GDPR). Potrivit Ghidului, "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”.

Listă exemplificativă cu acțiuni de întreprins pentru conformarea la GDPR

1. Analiza și identificarea datelor prelucrate de organizație, cu analiza scopului, temeiului și perioadei pentru care sunt reținute datele.
2. Analiza necesității unui DPO
3. Inițiere redactare Registrul Operațiunilor de Prelucrare
4. Redactare
    a. politică internă privind prelucrarea datelor personale în organizație.
    b. politică internă privind retenția datelor prelucrate de organizație.
    c. politică de informare a angajaților privind datele care le sunt prelucrate.
    d. politică de informare a clienților, vizitatorilor siteului etc.
    e. politică privind analiza interesului legitim și realizarea Data Protection Impact Assessment – Evaluare de Impact.
    f. politică internă privind arhitectura organizației din perspectiva prelucrării de date cu caracter personal (DPO, responsabil cu securitatea datelor, responsabili departamentali pentru diverse tipuri de prelucrări etc).
5. Training intern cu privire la prevederile GDPR pentru recunoașterea cererilor persoanelor vizate, a procedurii de urmat atunci când se primesc acestea, precum și a modului în care se dă răspunsul.
6. Politică internă privind metodele de identificare existente pentru persoanele vizate ale caror date sunt prelucrate.
7. Politică internă privind răspunsul la cererile persoanelor vizate (șabloane de răspuns, termen de răspuns etc.).
8. Politică tehnică privitoare la dreptul la portabilitatea datelor (în ce format se vor exporta datele, ce procedură se va urma etc.)
9. Procedură și formular de analiză a furnizorilor companiei (dacă respectă sau nu prevederile GDPR).
10. Contracte cu operatorii / împuterniciții cu care lucrați, din perspectiva operațiunilor de prelucrare a datelor cu caracter personal.
11. În funcție de specificul situației companiei dumneavoastră, mai pot există multe alte elemente a căror implementare să fie necesară (ex. Politică de prelucrare a datelor în contextul realizării testelor psihometrice în activitatea de HR a companiei etc.).

După cum se observă din expunerea de până acum, GDPR impune o **particularizare extremă a implementării sale în diverse entități**.

E foarte probabil ca, dacă luați de pe internet anumite acte tipizate, procedurile sau documentele preluate așa să facă mai mult rău decât bine procesului de implementare pe care îl construți. Puteți informa, spre exemplu, persoanele vizate, că au drepturi pe care nu le au, pentru că acele documente menționează situații care nu se întamplă în organizația dumneavoastră.

Alegeți cu grijă. Buna credință în implementarea GDPR, transparența prelucrărilor pe care le realizați, faptul că ați procedat la realizarea unor documente prin eforturi proprii, toate acestea vor constitui întotdeauna argumente valide pentru persoanele vizate ori pentru Autoritatea de Supraveghere.