

RESPONSABIL PROTECȚIA DATELOR (DPO)

**-SPECIALIZARE, EVALUARE, CERTIFICARE-
BLENDED-LEARNING**

Prelucrarea datelor cu caracter personal este prezentă aproape în orice activitate de afaceri, indiferent de industria în care activează operatorul de date sau împuternicitul acestuia. Mai ales pentru industriile care sunt caracterizate prin *operațiuni zilnice de prelucrări* ale datelor cu caracter personal (financiar – bancar, asigurări, IT&C, telecom, media, etc.), cunoașterea va deveni stringentă, deoarece noul pachet legislativ adoptat de Parlamentul și Consiliul European la începutul anului 2016, ce se va aplica începând cu data de **25 mai 2018**, cuprinde 2 acte normative semnificative:



- Regulamentul (UE) 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)
- Directiva (UE) 2016/680 referitoare la protecția datelor personale în cadrul activităților specifice desfășurate de autoritățile de aplicare a legii.

Poziția de "**responsabil cu protecția datelor**" a fost stabilită prin articolul 37 al Regulamentului General al UE privind protecția datelor, ca o măsură *obligatorie* pentru anumiți operatori de date și persoanele împuternicite de aceștia, în anumite cazuri, de ex. instituțiile publice sau în anumite situații date de circumstanțele operațiunilor, cum ar fi prelucrarea datelor sensibile pe scară largă, ori monitorizarea sistematică a persoanelor fizice ale căror date sunt prelucrate.

Deși această ocupație de responsabil cu protecția datelor (DPO) era deja existentă în sistemul legislativ al altor țări membre UE chiar înainte de apariția Regulamentului numărul 679/2016, este de observat că îndeplinirea sa necesită cunoștințe temeinice pentru înțelegerea tuturor operațiunilor de prelucrarea datelor personale, în contextul afacerii sau activității instituționale a operatorului sau a împuternicitului acestuia, a riscurilor pe care le implică operațiunile de prelucrare a datelor pentru persoanele vizate, respectiv a drepturilor și intereselor lor fundamentale, în echilibru cu interesele legitime ale operatorilor.

OBIECTIV

Cursul integrează elementele principale ale regimului juridic privind protecția datelor cu caracter personal, atât prin prisma legislației dreptului intern cât și al dreptului UE, având în centrul său Regulamentul General UE privind protecția datelor cu numărul 679/2016, dar și o legislație specială, care trebuie privită ca un sistem interdependent, în cele mai des întâlnite practici, cum ar fi comerțul electronic, prelucrarea datelor în mediul on-line, măsurile de verificare a integrității, cunoașterea clienței, cloud computing, crearea de profiluri, supravegherea video, măsurile de prevenire a actelor de spălare a banilor și de finanțare a terorismului etc.

GRUP ȚINTĂ

Persoanele desemnate să preia funcția de responsabil cu protecția datelor sau ofițer protecția datelor, persoanele din departamentele de conformitate, juridic, IT sau securitate IT, persoane având funcția de manager de proiect pentru proiectele care implică prelucrarea datelor personale la scara largă și care necesită o evaluare a impactului asupra protecției datelor, specialiști din departamentele de resurse umane sau alte departamente unde se realizează frecvent operațiuni de prelucrare a datelor cu caracter personal în diverse scopuri.

CONDIȚII DE ACCES

Participanții la curs trebuie să facă dovada că sunt absolvenți de studii superioare și prezintă acte de studii, în acest sens.

CONȚINUT

Modulul 1

- Legislația națională și a UE aplicabilă în domeniul protecției datelor, în coroborare cu Regulamentul General (UE) privind protecția datelor 679/2016;
- Coroborarea legislației din domeniul protecției datelor cu alte acte normative din alte domenii incidente, cum ar fi Codul Civil, Codul Muncii, Codul de procedură fiscală, Regulamentele Băncii Naționale a României (de ex. cunoașterea clienței) etc;
- Noțiunile de "prelucrare de date cu caracter personal", "date cu caracter personal", "categorii de date speciale", "numere de identificare națională", consimțământ "în forma scrisă sau în formă electronică";
- Noțiunile de "persoană vizată", "operator de date", "operatori asociați", "persoană împuternicită", "terț", "sub-contractor al persoanei împuternicite", "reprezentanții operatorilor sau ai împuterniciților care nu își au sediul în Uniune";
- Noțiunea de măsuri "tehnice și organizatorice";
- Noțiunea de teme juridic al prelucrării de date cu caracter personal și condițiile aplicabilității lor:
 - Consimțământul;
 - Încheierea sau executarea contractului;
 - Îndeplinirea unei obligații legale;
 - Interesul legitim;
 - Drepturile persoanei vizate;
 - Dreptul de informare;
 - Dreptul de acces la datele cu caracter personal;
 - Dreptul de rectificare și ștergere a datelor;
 - Dreptul la restricționarea datelor;
 - Dreptul la portabilitatea datelor;
 - Dreptul la opoziție;
 - Dreptul de a nu fi subiect al unei decizii individuale automate;
- Studii de caz și proiecte.



Modulul 2

- Rolul și responsabilitățile ofițerului de protecția datelor:
 - Fișa de post;
 - Obiective de performanță;
 - Colaborarea ofițerului de protecția datelor cu alte departamente.
- Registrele privind operațiunile de prelucrare a datelor personale;
- Protecția datelor cu caracter personal de la momentul conceperii: "Privacy by design and by default";
- Exercițiul de evaluare a impactului asupra protecției datelor:

- Cerințe și metode de evaluare a impactului asupra protecției datelor;
 - Riscurile evidențiate asupra protecției drepturilor fundamentale ale persoanei vizate și măsurile de diminuare a acestora;
 - Consultarea prealabilă cu autoritatea de supraveghere competentă;
 - Rolul ofițerului de protecția datelor în cadrul exercițiilor de evaluare a impactului asupra protecției datelor;
- Studii de caz și proiecte.

Modulul 3

- Relația contractuală dintre operatorul de date și persoana împuternicită;
- Misiunile de audit;
- Clauzele contractuale;
- Transferurile transfrontaliere/internaționale de date cu caracter personal;
- Stabilirea autorității de supraveghere principală/alte autorități de supraveghere competente;
- Reguli corporatiste obligatorii, codul de conduită, mecanismul certificării;
- Principiul responsabilității: răspunderea operatorului și a persoanei împuternicite;
- Răspunderea responsabilului de protecția datelor;
- Măsurile de protecție a responsabilului cu protecția datelor personale;
- Incidente de protecție și securitate a datelor;
- Planul de răspuns la incidentele de securitate a datelor;
- Stabilirea drepturilor și obligațiilor părților: persoana vizată, operatorul de date, persoana împuternicită de operatorul de date;
- Stabilirea circumstanțelor în care a intervenit incidentul de protecția datelor,
- Cooperarea dintre autoritatea de supraveghere principală și celelalte autorități de supraveghere în situația investigațiilor realizate de acestea;
- Răspunderea juridică și sancțiunile legale aplicabile;
- Studii de caz.

LECTORI

Maria Maxim este Partener Coordonator Practică Protecția Datelor la Wolf

Theiss România, filiala locală a uneia dintre cele mai importante firme de avocatură din Europa Centrală și de Est. Anterior, a fost Senior Manager în Departamentul de Investigare a Fraudelor și de Soluționare a Disputelor în România din cadrul EY Romania. A lucrat în industria de telecomunicații în mai multe posturi de conducere executivă, în domeniul protecției datelor, juridic precum și conformitate. A deținut funcția de director executiv de conformitate și director executiv de protecția datelor, făcând parte dintr-o echipă internațională.

Maria are o vastă experiență în domeniile juridic, de conformitate, anti-trust și protecția datelor. Ea este, de asemenea, avocat membru al Baroului București. Este certificată de Frankfurt School of Management ca și investigator de fraudă și deține Certificatul internațional avansat în Conformitate și Criminalitate Financiară, acordat de International Compliance Association (UK). A desfășurat numeroase proiecte internaționale în materie de conformitate, anti-trust, de protecția datelor, dreptul muncii, achiziții, dispute, litigii și investigații.



Nicolae Doicov este consultant protecției datelor și securității informației, cu experiență în domeniile: auditului cadrului GDPR pentru diferite companii de marketing on-line, elaborării Jurnalului de înregistrări al operațiunilor cu caracter personal pe baza rezultatelor auditului, emiterii documentației specifice privind confidențialitatea datelor pentru alinierea la cerințele RGPD, auditului cadrului ISMS și propunerea soluției pentru implementare și manager de proiect în ceea



ce privește: coordonarea evaluării și implementării cadrului GDPR, participarea la fazele de audit cu avocații, efectuarea de interviuri pentru identificarea operațiunilor de prelucrare a datelor, compilarea constatărilor rezultate din analizele non-conformităților și crearea unui plan de acțiune pentru implementare în consecință. A condus pentru ERICSSON Telecommunication Romania gestionarea proiectului în legătură cu încadrarea a 200 de persoane în servicii și activități la nivelul Global Service Center. A mai derulat proiecte pentru Huawei Technologies Romania, Telemobile Zapp Romania, etc. Detine, printre altele, certificări ISO27001- Managementul Securității Informației – Top Quality Management, PRINCE 2 Foundation & Practitioner - IT Academy, ITIL Service Operations, ITIL Foundation.

DURATA CURSULUI/PERIOADA DE DESFĂȘURARE

Cursul se va desfășura pe parcursul a **două luni** de pregătire (aprilie-iunie 2019), cu trei sesiuni la clasă și studiu individual, astfel:

Ziua 1: **19 aprilie 2019**, în intervalul orar 9-18;

Ziua 2: **17 mai 2019**, în intervalul orar 9-18;

Ziua 3: **3 iunie 2019**, în intervalul orar 9-18.

Program de studiu recomandat:

Ore la clasă: 30

Ore pentru realizarea celor două proiecte intermediare, inclusiv studiu individual: 75

Ore pentru elaborarea proiectului individual final, inclusiv studiu individual: 75

Total: 180 ore

EVALUARE

Materiale de studiu: suportul de curs și bibliografia recomandată de lector.

După finalizarea modulelor 1 și 2, participanții vor pregăti două **proiecte intermediare**, de grup.

Evaluarea finală se va organiza în data de **21 iunie 2019** și va consta în prezentarea unui proiect, ce va fi susținut în fața unei *comisii de examinare și evaluare* compusă din: Maria Maxim, ICA – Managing Partner, Wolf Theiss România, Doru Bebe Bulată, ICA, ACAMS – Consilier Președinte - Guvernanță Corporativă, Risc, Conformitate, EximBank și Președinte Comisia de Conformitate, Asociația Română a Băncilor și Dr. Gabriela Hârțescu, Director General, Institutul Bancar Român.

La finalizarea cu succes a cursului, participanților li se va elibera un Certificat de Absolvire, emis de IBR (sub egida membrilor fondatori: BNR și ARB).

TAXA DE PARTICIPARE

Tariful cursului este **600 EUR/participant***, cu posibilitatea achitării în 2 rate astfel:

- 300 EUR - rata 1, până în data de 18 aprilie 2019
- 300 EUR - rata 2, până în data de 3 iunie 2019.

Detalii cu privire la derularea programului și a procedurilor de înscriere pot fi obținute la adresa de e-mail: sanda.voinescu@ibr-rbi.ro; telefon **0372 394442**, mobil **0748 886 820**.

* Nu se aplică TVA. Plata primei rate se va face integral, **cu cel puțin patru zile înainte de începerea cursului**, în contul Institutului Bancar Român numărul RO93BTRLRONCRT0261315401, deschis la Banca Transilvania, Sucursala Lipskani (pe ordinul de plată va rugăm să specificați numele cursanților și titlul cursului). În cazul în care un participant anunță retragerea sa de la curs cu 1-2 zile înainte de începerea cursului, din suma plătită **se reține un procent de 17 %**. În cazul în care un participant anunță retragerea la data începerii cursului, suma plătită **nu se mai restituie**. În toate cazurile, există posibilitatea înlocuirii participantului retras cu un alt participant, caz în care nu se percepe nici o penalizare.