CE ÎNSEAMNĂ PENTRU DVS. NOILE REGLEMENTĂRI UE PRIVIND PROTECȚIA DATELOR?

Regulamentul general pentru protecția datelor

Document informativ pentru IMM-uri

Această publicație reprezintă o traducere a unui document publicat inițial de Accountancy Europe în aprilie 2017, intitulat *What do the new EU data protection rules mean for you?*.

Traducerea a fost realizată în întregime sub răspunderea CECCAR. Accountancy Europe nu își asumă nicio responsabilitate pentru conținutul documentului și acuratețea traducerii. În cazul unor neclarități, cititorul trebuie să consulte versiunea originală în limba engleză, care poate fi descărcată gratuit de pe website-ul Accountancy Europe.

FACTS.

PROBLEME PROFESIONALE
APRILIE 2017

ASPECTE PRINCIPALE

Noile reglementări UE privind protecția datelor vor intra în vigoare la 25 mai 2018 și se vor aplica tuturor entităților care utilizează informații cu caracter personal, indiferent dacă sunt păstrate în format electronic sau tipărit. Profesioniștii contabilii sunt direct afectați de aceste dispoziții deoarece aceștia colectează, stochează și procesează date cu caracter personal legate de clienți, angajați și subcontractori. Aceste dispoziții referitoare la protecția datelor trebuie tratate cu atenție, deoarece amenzile ar putea ajunge la zeci de milioane de Euro.

Scopul acestui document informativ este de a ajuta contabilii să înțeleagă modul în care noua legislație le afectează activitatea. Vom explica modificările legislative și vom prezenta exemple privind ceea ce înseamnă acestea în practică, de exemplu: informarea clienților cu privire la drepturile lor, asigurarea unei securități cibernetice adecvate și o reacție mai bună și mai promptă la încălcarea securității datelor.

INTRODUCERE

Profesia contabilă trebuie să se pregătească cu atenție pentru *Regulamentul General privind Protecția Datelor* (GDPR)[1], care intră în vigoare de la 25 mai 2018. Acesta stabilește cadrul legal obligatoriu pentru protecția datelor personale în interiorul UE. Practicienii din domeniul contabil procesează date cu caracter personal și, prin urmare, sunt afectați direct de această legislație. GDPR se bazează pe și înlocuiește *Directiva UE privind protecția datelor*[2] (Directiva) adoptată cu 21 de ani în urmă.

Modul în care datele personale sunt comunicate și utilizate s-a modificat față de 1995. Prin urmare, noua legislație are un dublu obiectiv – (i) de a lua în considerare aceste modificări din domeniul datelor personale și (ii) de a asigura un cadru general de reglementare mai consecvent la nivelul UE. În acest scop, GDPR introduce o serie de obligații oneroase noi și penalizări sporite în caz de neconformitate.

Toate organizațiile care lucrează cu informații cu caracter personal trebuie să-și revizuiască procedurile în cel mai scurt timp posibil pentru a se asigura că se conformează noilor prevederi. Un studiu finanțat de Google estimează un cost mediu anual de până la 7.200 de euro[3] pentru implementarea GDPR de către o IMM obișnuită.

Această publicație începe cu o scurtă prezentare a principalelor concepte din domeniul protecției datelor. Sunt discutate apoi principiile majore prescrise de GDPR pentru procesarea datelor personale. A treia parte a publicației include aspecte legate de supraveghere și de neconformitatea cu GDPR. Înainte de a concluziona prin prezentarea principalelor modificări determinate de GDPR, sunt trecute în revistă câteva aspecte legate de transferul datelor personale către terțe țări.

CONCEPTE CHEIE ȘI ROLUL PRACTICIENILOR ÎN PROTECȚIA DATELOR

Datele personale includ orice informații referitoare la o persoană fizică identificabilă (persoana vizată). De exemplu, adresa de domiciliu, venitul sau numărul de telefon al unei anumite persoane. Practicienii din domeniul contabilității procesează în mod regulat datele personale ale clienților sau angajaților lor.

Procesarea datelor reprezintă orice operațiune efectuată asupra datelor personale. Aceasta include colectarea, înregistrarea, structurarea, stocarea, adaptarea, consultarea, utilizarea, divulgarea, ștergerea sau distrugerea datelor.

---

[1] Regulamentul (UE) 2016/679, disponibil pe: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[2] Directiva 95/46/CE, disponibilă pe: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l14012&from=EN

[3] L. Christensen, A. Colciago, F. Etro și G. Rafert, *Impactul Regulamentului privind protecția datelor în UE* (13 februarie 2013), disponibil pe: http://bit.ly/2iTWy9r

De exemplu, contabilii colectează și stochează informații referitoare la identitatea unui nou client pentru a se conforma dispoziţiilor de verificare prealabilă a clienților din *Directiva privind combaterea spălării banilor*. Atunci când furnizează servicii de salarizare clienților lor (și lor înșiși), au acces, de asemenea, la date personale relevante ale angajaților. Auditorii procesează datele personale ale angajaților clienților lor.

Datele pot fi procesate de operatori de date sau persoane împuternicite de operatori. Operatorii de date determină obiectivele și mijloacele de procesare a datelor personale. Operatorii de date pot apela la împuterniciți care să proceseze datele personale în numele lor. Operatorii de date trebuie să țină cont de responsabilitățile pe care le au atunci când lucrează cu un împuternicit.

Practicienii pot fi atât operatori de date, cât și împuterniciți. De exemplu, un contabil care stochează în cloud datele personale ale clienților lor este un operator de date. Furnizorul de servicii cloud este, în acest caz, un împuternicit care procesează datele stocate de operatorul de date. Totuși, contabilul își păstrează responsabilitățile atunci când externalizează activitatea de procesare a datelor, inclusiv în ceea ce privește asigurarea unei securități corespunzătoare a datelor personale.

GDPR nu acoperă procesarea datelor personale de către o persoană fizică în decursul unei activități personale sau domestice. De asemenea, acesta nu include informațiile referitoare la corporații sau alte entități juridice, adică informații nepersonale.

De exemplu, practicienii nu intră în aria de acoperire a GDPR atunci când procesează informații referitoare la locul de desfășurare a activității clientului lor (informație nepersonală) sau când țin evidența notelor primite de copiii lor (activitate domestică).

PRINCIPII DE PROCESARE A DATELOR PERSONALE

Operatorii de date determină obiectivele și mijloacele de procesare a datelor personale. Această secțiune detaliază condițiile în care datele personale pot fi procesate în mod legal, ce trebuie avut în vedere pentru a respecta drepturile persoanelor vizate și modul în care operatorii de date și persoanele împuternicite de operatori trebuie să poată dovedi că își respectă obligațiile.

MOTIVE PENTRU PROCESAREA DATELOR PERSONALE

Procesarea datelor personale este legitimă atunci când este necesară pentru:

- a îndeplini un contract la care persoana vizată este parte
- a se conforma cu o obligaţie legală

- a proteja interesele vitale ale persoanei vizate
- a realiza o sarcină în interesul public sau în exercitarea competențelor oficiale
- a urmări interesele legitime ale operatorului de date – cu excepția situației în care acestea se opun drepturilor fundamentale ale persoanei vizate

De exemplu, practicienii pot justifica procesarea informațiilor personale ale clienților, în contextul procesului de verificare prealabilă a clienților, ca având scopul de a executa o sarcină în interesul public și de a se conforma obligațiilor lor în baza legislației pentru combaterea spălării banilor.

În afară de opțiunile menționate mai sus, procesarea datelor este, de asemenea, posibilă atunci când persoana vizată își dă acordul. Totuși, condițiile în care este posibil acest lucru sunt reglementate strict, iar operatorul de date trebuie să poată demonstra că persoana vizată și-a dat acordul pentru procesare. Un aspect important, furnizarea unui serviciu nu impune exprimarea acordului în cazul în care procesarea nu este necesară pentru furnizarea acelui serviciu. Mai mult, persoana vizată își poate retrage acordul în orice moment.

De asemenea, GDPR introduce reguli pentru situațiile în care datele personale sunt procesate în scopuri ce depășesc scopul inițial. Acesta impune operatorilor de date să documenteze corespunzător această decizie și să descrie factorii avuți în vedere în luarea acestei decizii.

DREPTURI DE PROTECȚIE A DATELOR

Practicienii vor trebui să informeze persoanele vizate de la care colectează informații personale, cum ar fi clienții, cu privire la drepturile lor de protecție a datelor și să ia măsuri în vederea facilitării acestor drepturi. Acest lucru ar putea necesita revizuirea informațiilor furnizate persoanelor vizate cu privire la modul în care sunt procesate datele lor personale. O astfel de revizuire trebuie să includă o analiză a măsurii în care limbajul folosit este clar și inteligibil pentru persoanele vizate[4].

Drepturile de protecție a datelor includ dreptul la rectificare, opunere, ștergere, acces, portabilitate, restricționarea procesării și anumite drepturi legate de crearea profilelor – o parte din aceste drepturi sunt descrise mai jos. Se recomandă practicienilor implicați în analizarea unor volume mari de date să studieze noile prevederi referitoare la realizarea de profiluri, aceasta fiind considerată o activitate cu grad ridicat de risc[5].

De asemenea, practicienii trebuie să acționeze și să răspundă la orice solicitare a unei persoane vizate, cum ar fi clienții, de a-și exercita drepturile. Aceasta ar putea

[4] Hogan Lovells, *Adaptarea la cerințele viitorului în domeniul confidențialității: Un ghid de pregătire pentru Regulamentul UE privind Protecția Datelor*.
[5] Hogan Lovells, *Adaptarea la cerințele viitorului în domeniul confidențialității: Un ghid de pregătire pentru Regulamentul UE privind Protecția Datelor*.

implica elaborarea unor proceduri noi pentru tratarea unor astfel de solicitări. În plus, cu excepția cazului în care solicitările persoanei vizate sunt vădit nefondate sau excesive, practicienii trebuie să realizeze gratuit orice acțiuni legate de drepturile acesteia în domeniul protecției datelor. Dacă nu se ia nicio măsură ca răspuns la o solicitare, practicianul trebuie să informeze persoana vizată cu privire la drepturile acesteia de a depune o plângere.

Obligațiile în domeniul protecției datelor descrise mai sus se aplică, de asemenea, în ceea ce privește informațiile referitoare la angajați. Statele membre sau acordurile colective între angajați și angajatori pot adopta mai multe reguli pentru procesarea datelor personale ale angajaților în contextul activității lor ca angajați. Acest lucru înseamnă că ar putea exista diferențe în dispoziţii de la un stat membru la altul.

DREPTUL LA INFORMARE

Atunci când datele sunt colectate direct de la persoana vizată, operatorul de date trebuie să ofere informații precum datele sale de contact, durata păstrării datelor, scopul procesării acestora și baza legală. Astfel, operatorii de date trebuie să furnizeze persoanei vizate (de exemplu, client, angajat etc.) răspunsuri clare la următoarele întrebări:

- cine ești?
- cine (altcineva) mai primește datele mele?
- de ce îmi procesezi datele?
- cât timp îmi vei păstra datele?
- care sunt drepturile mele în ceea ce privește protecția datelor?

Operatorul de date trebuie, de asemenea, să informeze persoanele vizate atunci când intenționează să proceseze suplimentar datele în alt scop decât cel pentru care au fost colectate inițial. Atunci când datele personale nu au fost colectate direct de la persoana vizată, operatorii de date trebuie să furnizeze persoanei vizate informații similare cazului în care datele sunt colectate direct.

De exemplu, pe parcursul procesului de verificare prealabilă a clienților, practicienii trebuie să le furnizeze clienților datele lor de contact și să le explice că informațiile lor sunt colectate în vederea realizării unei sarcini în interesul public. Atunci când un practician folosește un furnizor de servicii cloud ale cărui servere sunt în afara UE, acesta trebuie să informeze, în plus, clientul despre acest aspect și despre orice măsuri de protecție implementate în vederea protejării drepturilor acestuia.

DREPTUL LA ȘTERGEREA DATELOR

Dreptul la ștergerea datelor sau „dreptul de a fi uitat” impune operatorilor de date să șteargă datele personale la solicitarea persoanei vizate, în anumite circumstanțe. Dreptul la ștergerea datelor nu se aplică în cazul în care procesarea este necesară pentru a permite operatorului de date să se conformeze unor dispoziții legale sau în cazul în care procesarea este realizată în interesul public.

De exemplu, clienții nu pot solicita ștergerea informațiilor personale colectate în contextul procesului de verificare prealabilă a clienților.

RĂSPUNDERE

Operatorii de date trebuie să implementeze măsurile necesare pentru a se asigura și pentru a putea demonstra că procesarea datelor este în întregime conformă cu dispozițiile GDPR. Obligațiile ar putea fi îndeplinite prin aderarea la o procedură corespunzătoare de certificare sau la un cod de conduită. Teoretic, acest lucru implică, de asemenea, ca organizația să aibă proceduri documentate și evidențe referitoare la deciziile specifice. În plus, operatorii de date trebuie să realizeze o analiză de impact în domeniul protecției datelor înainte de a se angaja într-o activitate de procesare care este probabil să implice un grad ridicat de risc față de drepturile și libertățile persoanelor vizate. Pentru a se asigura conformarea la GDPR, este important să se meargă mai departe de un exercițiu de tip „bifați căsuța” și să se construiască o cultură corespunzătoare de protecție a datelor.

O nouă dispoziție a GDPR este faptul că operatorul are obligația de a lua măsuri care conduc la „protecția datelor din fața de concepție și protecția implicită a datelor”[6] și de a se asigura că sunt procesate doar datele personale strict necesare. De exemplu, în contextul verificării prealabile a clienților, practicienii nu trebuie să proceseze date personale, cum ar fi preferințele politice ale clientului.

Operatorii de date au obligația de a ține evidența activităților de procesare, inclusiv detalii ale măsurilor de securitate tehnice și organizaționale care vizează datele și protecția acestora. Totuși, există o derogare pentru organizații cu mai puțin de 250 de angajați.

Atât operatorii de date, cât și persoanele împuternicite de operatori trebuie să desemneze un responsabil cu protecția datelor în anumite situații. De exemplu, este necesar un responsabil cu protecția datelor atunci când activitățile principale ale organizației necesită o monitorizare permanentă și sistematică a persoanelor vizate la scară mare sau când acestea constau în procesarea la scară mare a unor date

[6] Pentru mai multe informații și îndrumări, a se vedea ENISA, *Confidențialitate încă din faza de concepție*, disponibil la: https://www.enisa.europa.eu/topics/data-protection/privacy-by-design

speciale sau a unor date legate de condamnări penale. Responsabilul cu protecția datelor trebuie să fie un specialist în domeniul protecției datelor și să monitorizeze conformitatea cu GDPR. Responsabilul poate fi un angajat al organizației, dat trebuie să fie independent în executarea activităților sale.

Principiul răspunderii asupra datelor se extinde, de asemenea, la interacțiunea cu persoanele împuternicite de operatorii de date. GDPR impune operatorilor să utilizeze doar împuterniciți care ofere suficiente garanții pentru a implementa măsuri corespunzătoare pentru a îndeplini cerințele GDPR. Acest lucru înseamnă că operatorii trebuie să își cunoască atât propriile obligații, cât și pe cele ale persoanelor împuternicite.

În afară de prevederile care afectează în egală măsură operatorii și persoanele împuternicite de aceștia, există dispoziții speciale care vizează persoanele împuternicite. De exemplu, se interzice unui împuternicit să implice un alt împuternicit fără acordul prealabil explicit al operatorului.

Contractul cu persoana împuternicită trebuie să stabilească limitele activității de procesare a datelor. Acesta trebuie să stipuleze că împuternicitul va asista operatorul în vederea conformării cu o serie de obligații ale acestuia din urmă, cum ar fi îndeplinirea solicitărilor persoanelor vizate, notificarea cazurilor de încălcare a securității datelor sau notificarea operatorului în cazul în care împuternicitul consideră că o anumită instrucțiune de procesare va încălca GDPR.

Noile obligații aplicabile operatorilor de date și persoanele împuternicite de operatori vor afecta relațiile contractuale viitoare dintre operatori și persoanele împuternicite. Prin urmare, contractele vor deveni, probabil, mai detaliate. Noile obligații ar putea impune, de asemenea, o revizuire a contractelor existente[7].

Practicienii trebuie să fie deci atenți atunci când utilizează furnizori, cum ar fi furnizorii de servicii cloud. Acest aspect poate fi avut în vedere încă de la selectarea furnizorului. De exemplu, atunci când lansează o invitație la licitație pentru un serviciu cloud, practicienii pot include în invitație criterii legate de modul în care împuternicitul tratează securitatea cibernetică sau de existența unui raport de certificare privind conformitatea cu standardele internaționale relevante.

[7] Hogan Lovells, *Adaptarea la cerințele viitorului în domeniul confidențialității: Un ghid de pregătire pentru Regulamentul UE privind Protecția Datelor*.

PROTECȚIA DATELOR SE APLICĂ ȘI ÎN CAZUL FIȘETELOR

Biroul Comisarului pentru informații al Marii Britanii (UK), autoritatea care susține drepturile legate de informații în UK, a amendat Consiliul Comitatului Norfolk (Norfolk) pentru neconformarea la regulile de protecție a datelor[8].

Ca parte a mutării unui sediu, Norfolk a renunțat la o parte din mobilier, inclusiv fișete utilizate de echipa de asistență socială pentru copii. Norfolk nu a avut o procedură scrisă care se determine cine era responsabil de golirea fișetelor, care nu a fost realizată. Ca urmare, o persoană care a cumpărat o parte din mobilier a primit dosare care cuprindeau informații sensibile.

ICO a descoperit că Norfolk nu avea implementate măsuri corespunzătoare împotriva procesării neautorizate de date personale și împotriva pierderii accidentale sau distrugerii datelor personale. Norfolk a primit o amendă de 60.000£.

Acest caz demonstrează importanța existenței unor proceduri corespunzătoare de protecție a datelor, indiferent dacă utilizezi servicii cloud sau suport hârtie.

SECURITATE

Atât operatorul, cât și persoana împuternicită de acesta trebuie să implementeze măsuri corespunzătoare pentru a asigura un nivel adecvat de securitate. Astfel de măsuri trebuie să se bazeze pe o evaluare a riscurilor.

GDPR impune atât operatorului, cât și persoanei împuternicite să ia în considerare actualele „tehnologii de ultimă generație” atunci când implementează măsuri de securitate și menționează în mod specific pseudo-anonimizarea și criptarea ca tehnici ce ar putea fi aplicate. Acest lucru va pune mai multă presiune pe organizații să analizeze cel puțin dacă aceste măsuri sunt necesare și eficiente din punct de vedere al costurilor și, dacă da, să le implementeze.

Implementarea unor astfel de măsuri tehnice este rareori simplă. De exemplu, criptarea este improbabil să fie eficientă în cazul în care datele sunt transferate către un serviciu online (cum ar fi un pachet de contabilitate), în timp ce pseudo-anonimizarea ar putea fi potrivită, însă doar în urma unei adaptări. Prin urmare, implementarea unor astfel de măsuri va avea implicații legate de costuri.

GDPR introduce, de asemenea, noi reguli în ceea ce privește reacțiile în cazul încălcării securității datelor. Într-o astfel de situație, operatorii au obligația de a raporta încălcarea către autoritatea de supraveghere competentă, de îndată ce este posibil. În cazul în care încălcarea prezintă un risc ridicat față de drepturile și

[8] ICO, disponibil la: https://ico.org.uk/media/action-weve-taken/mpns/2013720/mpn-norfolk-county-council-20170315.pdf

libertățile persoanelor vizate, operatorii de date trebuie să notifice, de asemenea persoanele vizate cu privire la această încălcare. Obligația persoanei împuternicite de operator este de a notifica fără întârziere operatorul cu privire la orice încălcare a securității datelor.

De exemplu, dacă cineva accesează ilegal serverul unui practician și fură informații personale ale clienților (cum ar fi parole, adrese de domiciliu, vârstă și câștiguri), atunci practicianul trebuie să raporteze această încălcare a securității datelor către autoritatea de supraveghere și clienții săi[9]. Dacă un practician stochează datele clienților în cloud, atunci furnizorul de servicii cloud va trebui să informeze practicianul cu privire la orice încălcare a securității datelor. Acesta din urmă trebuie să notifice apoi autoritățile de supraveghere și clientul.

ÎNDRUMĂRI PRIVIND SECURITATEA DATELOR DISPONIBILE PENTRU IMM-URI

Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) a publicat îndrumări pentru a ajuta IMM-urile să adopte o abordare bazată pe riscuri pentru securitatea datelor personale pe care le procesează[10].

Îndrumările au scopul de a ajuta IMM-urile să înțeleagă contextul procesării datelor personale și să evalueze singure, prin intermediul unui chestionar, riscurile de securitate asociate. ENISA propune, de asemenea, măsuri de securitate organizaționale și tehnice care ar putea fi adoptate de IMM-uri în vederea conformării cu GDPR.

IMPLEMENTAREA GDPR

SUPERVIZARE

GDPR introduce conceptul de „autoritate de supraveghere principală”. Această autoritate este organismul de supraveghere al statului membru în care este localizat sediul principal din UE al operatorului sau persoanei împuternicite de operator. Această autoritate va lua inițiativa în cazul tuturor activităților de procesare transfrontaliere realizate de organizația respectivă – practic, un „punct central” pentru organizație pentru toate activitățile de procesare din interiorul UE.

Autoritățile de supraveghere ale altor state membre decât cel în care este localizată autoritatea de supraveghere principală ar putea fi totuși implicate în cazul în care activitățile de procesare ale unei organizații afectează un stat membru. Această situație se întâlnește, de exemplu, atunci când există activități de procesare exclusiv

[9] Puteți verifica dacă aveți un cont compromis în urma unei încălcări a securității datelor aici: https://haveibeenpwned.com/
[10] ENISA, *Îndrumări pentru IMM-uri cu privire la securitatea procesării datelor personale*, (ianuarie 2017), document disponibil pe: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

în ceea ce privește persoane din interiorul granițelor naționale ale acelui stat membru.

Aceasta ar putea reprezenta o schimbare valoroasă pentru operatorii sau persoanele împuternicite de operatori care au sedii în mai multe state membre, deoarece ar trebui să simplifice cerințele de înregistrare, legale și de raportare care le vizează. Prin urmare, aceste entități sunt încurajate să identifice cine este autoritatea de supraveghere principală în cazul lor.

De exemplu, o rețea de audit va trebui să colaboreze, în principal, cu autoritatea de supraveghere aferentă sediului său principal din UE. În cazul în care un practician dintr-o rețea ia măsuri pentru a se conforma cu o decizie emisă de autoritatea de supraveghere principală, acesta trebuie să notifice doar autoritatea de supraveghere principală cu privire la aceste acțiuni. Aceasta din urmă va notifica apoi celelalte autorități de supraveghere implicate.

Statele membre pot reglementa suplimentar competențele autorităților de supraveghere în raport cu operatorii de date și persoanele împuternicite de aceștia, care fac obiectul regulilor referitoare la secretul profesional.

NECONFORMITATEA

Anumite încălcări ale securității datelor pot avea ca rezultat amenzi care se ridică până la valoarea cea mai mare dintre 20 de milioane de euro și 4% din cifra de afaceri la nivel global. Încălcările mai puțin grave pot avea ca rezultat amenzi care se ridică până la valoarea cea mai mare dintre 10 milioane de euro și 2% din cifra de afaceri la nivel global. În majoritatea statelor membre, GDPR va conduce, probabil, la o creștere semnificativă a potențialelor sancțiuni pentru încălcarea drepturilor persoanelor vizate.

Persoanele vizate vor avea drepturi suplimentare, cum ar fi dreptul de a depune o plângere la autoritatea de supraveghere, dreptul de a acționa în justiție un operator sau un împuternicit și dreptul de a obține o despăgubire de la operator.

TRANSFERUL DATELOR PERSONALE CĂTRE TERȚE ȚĂRI

Datele personale pot fi transferate țărilor din afara UE doar dacă se poate garanta același nivel de protecție. În practică, acest lucru înseamnă fie că țara respectivă trebuie să aibă un cadru general similar de protecție a datelor ca UE, fie că operatorii de date trebuie să se asigure că sunt adoptate anumite măsuri pentru a garanta o protecție suficientă a datelor.

Comisia Europeană evaluează nivelul de protecție disponibil în terțe țări și ține o evidență a tuturor celor care îndeplinesc criteriile. Se pot face transferuri de date către oricare din țările terțe de pe listă fără a fi necesară o autorizare explicită. Până

în acest moment, doar câteva țări au demonstrat un nivel adecvat de protecție și au fost incluse pe lista Comisiei Europene[11].

Datele personale pot fi trimise totuși către terțe țări neechivalente dacă sunt asigurate măsuri de protecție corespunzătoare. Aceste măsuri de protecție pot lua forma unor reguli corporative obligatorii, a unor clauze contractuale standard aprobate de Comisie, sau a unor coduri de conduită sau proceduri de certificare aprobate.

Practicienii nu vor avea nevoie de autorizare pentru a stoca date în Elveția, care este pe lista Comisiei. Pe de altă parte, dacă o rețea de audit dorește să își stocheze datele în Islanda, poate face acest lucru prin adoptarea unor reguli corporative cu caracter juridic obligatoriu. Astfel de reguli trebuie să includă acceptarea răspunderii de către entitățile cu sediul în UE pentru orice încălcări săvârșite de membri din afara Uniunii.

TRANSFERURI CĂTRE MAREA BRITANIE (UK): EFECTELE BREXIT-ULUI

Atunci când UK (sau un alt stat membru) va pleca din UE, acesta va fi considerat o „țară terță". Acest lucru înseamnă că operatorii de date din UK și împuterniciții acestora care procesează date personale de la persoane din interiorul Uniunii Europene sau operatorii de date din UE care utilizează împuterniciți ce transferă date către UK vor trebui să își revizuiască practicile actuale de procesare a datelor[12].

TRANSFERURI CĂTRE STATELE UNITE (SUA): SCUTUL DE CONFIDENȚIALITATE

SUA constituie un caz special. Este permis transferul de date de la companii din UE către companii din SUA atunci când companiile din SUA fac parte din *Scutul de confidențialitate*[13]. Atunci când practicienii doresc să mute datele personale ale clienților în SUA sub acoperirea Scutului de confidențialitate, trebuie să se asigure că acele companii din SUA cu care colaborează sunt incluse pe lista Scutului de confidențialitate și că au luat toate măsurile necesare pentru a se conforma dispozițiilor. Altfel, pot transfera date atunci când utilizează alte mijloace autorizate pentru a asigura o protecție corespunzătoare a datelor (de exemplu, prin intermediul unor clauze contractuale).

[11] Comisia Europeană, *Deciziile Comisiei cu privire la gradul de adecvare a protecției datelor personale în terțe țări*, disponibile la: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[12] GDPR devin aplicabil din mai 2018. Acest lucru înseamnă că dacă negocierile pentru Brexit nu vor fi finalizate până atunci, UK va trebui să respecte GDPR până la finalizarea Brexit-ului.

[13] Comisia Europeană, *Scutul de confidențialitate UE-SUA*, disponibil pe: http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

Scutul de confidențialitate UE-SUA este criticat în prezent deoarece nu ar furniza o protecție suficientă a datelor personale. Atunci când predecesorul *Scutului de confidențialitate*, *Acordul privind sfera de securitate*, a fost invalidat, s-a creat o incertitudine juridică majoră pentru firmele de contabilitate și audit care utilizau servere din SUA. Prin urmare, se recomandă practicienilor care își stochează datele în SUA să ia în calcul acest aspect și să urmărească orice evoluții relevante anunțate de Comisia Europeană, precum și modificările din politicile SUA referitoare la date.

CONCLUZIE

Această publicație a descris câteva dintre principalele obligații conform GDPR care s-ar putea aplica practicienilor atunci când procesează date personale. Este probabil ca aceste reguli noi să impună o revizuire a procedurilor existente de procesare a datelor. Se recomandă practicienilor să se asigure că dețin expertiza necesară atunci când fac acest lucru.

Este probabil ca instituțiile europene și autoritățile de protecție a datelor să publice, dacă nu au publicat deja, îndrumări privind conformarea cu GDPR. Vă recomandăm să citiți cu atenție orice recomandări publicate de autoritățile dvs.

De exemplu, Grupul de lucru Art. 29 al UE, care este format din autoritățile naționale de protecție a datelor, a publicat îndrumări ce vizează responsabilii cu protecția datelor, portabilitatea datelor și modul în care poate fi identificată autoritatea dvs. de supraveghere principală[14]. În plus, Comisia Belgiană pentru Confidențialitate a publicat o broșură cu 13 pași în vederea conformării la GDPR[15].

PRINCIPALELE MODIFICĂRI ADUSE DE GDPR

Printre principalele modificări comparativ cu Directiva se numără:

- includerea operatorilor de date și a persoanelor împuternicite de operatori care dețin informații personale ale unor cetățeni europeni
- noi obligații referitoare la răspundere pentru operatorii de date
- noi drepturi referitoare la datele personale pentru persoanele vizate
- reglementări mai stricte pentru procesarea pe baza acordului persoanelor vizate
- unele organizații vor avea obligația de a desemna un responsabil cu protecția datelor
- reguli mai stricte privind încălcarea securității datelor
- introducerea unui „punct central” pentru activitățile de supraveghere
- notificarea sau aprobarea prealabilă de la Agenția pentru Protecția Datelor a fost eliminată în mai multe situații
- introducerea unor obligații directe pentru operatorii de date

[14] Grupul de lucru UE pentru Articolul 29, disponibil pe: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
[15] Comisia Belgiană pentru Confidențialitate, *Plan în 13 etape*, disponibil pe: https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf

Avenue d'Auderghem 22-28, 1040 Brussel

+32(0)2 893 33 60

www.accountancyeurope.eu

@AccountancyEU

Accountancy Europe

DESPRE ACCOUNTANCY EUROPE

Accountancy Europe reunește 50 de organisme profesionale din 37 de țări europene care reprezintă aproape 1 milion de profesioniști contabili, auditori și consultanți. Toți aceștia fac ca cifrele să lucreze în beneficiul oamenilor. Accountancy Europe transpune experiența sa zilnică în contribuții la dezbaterile de politică publică din Europa și dincolo de granițele acesteia.

Accountancy Europe este inclusă în Registrul pentru Transparență al UE (nr. 4713568401-18).