

CE DATE COLECTĂM ȘI UNDE LE PUTEM TRANSFERA?

Consecințe ale Deciziei CJUE în cazul Schrems privind
sistemul Safe Harbour

Alexandru Câmpean
29 octombrie 2015

TOPICS

- 1.CE DATE PRELUCRĂM?
- 2.LIMITELE ÎN CARE SE POATE DESFĂȘURA MONITORIZAREA
- 3.TRANSFERUL DATELOR ANGAJAȚILOR
- 4.SCHIMBĂRI IMINENTE ÎN CADRUL LEGAL



CATEGORII DE DATE

- **DATE CU CHARACTER PERSONAL:** acestea includ informații cum sunt numele și datele de contact ale angajatului, detaliile contului bancar, detalii privind salariul, etc.
- **CATEGORII SPECIALE DE DATE:** acestea privesc informațiile privind originea rasială sau etnică, convingerile politice, religioase, filozofice sau de natură similară, de apartenență sindicală, precum și informațiile privind starea de sănătate sau viața sexuală.

PRELUCRAREA DATELOR CU CARACTER PERSONAL

- UNDE?
- CUM?
- DE CE?

* „prelucrarea datelor cu caracter personal” înseamnă „orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automate sau neautomate, cum ar fi **colectarea, înregistrarea**, organizarea, **stocarea, adaptarea ori modificarea**, extragerea, consultarea, utilizarea, dezvăluirea către terți prin transmitere, diseminare sau in orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea”.

LIMITELE MONITORIZĂRII ANGAJAȚILOR

- Angajatorul care intenționează să își monitorizeze angajații va trebui să notifice acest fapt către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
- Informarea angajaților
- Consimțământul expres al angajaților trebuie obținut.

SMARTER
QUICKER
SHARPER

CADRUL LEGAL APLICABIL

LEGISLAȚIE NAȚIONALĂ

- Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

DREPT EUROPEAN

- Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestora;
- Decizia 2001/497/CE privind clauzele contractuale standard pentru transferul de date cu caracter personal către țările terțe în temeiul Directivei 95/46/CE; și
- Decizia 2010/87/UE privind clauzele contractuale tip pentru transferul de date cu caracter personal către persoanele împuternicite de către operator stabilite în țări terțe în temeiul Directivei 95/46/CE a Parlamentului European și a Consiliului

CONVENȚII INTERNAȚIONALE LA CARE ROMÂNIA ESTE PARTE:

- Declarația Universală a Drepturilor Omului;
- Convenția nr. 108 din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal;
- Convenția pentru apărarea drepturilor omului și a libertăților fundamentale (Convenția Europeană a Drepturilor Omului).

PRINCIPII ȘI LIMITE

GRUPUL DE LUCRU ARTICOLUL 29 STABILESTE URMATOARELE PRINCIPII:

- Principiul necesității
- Principiul finalității
- Principiul transparenței
- Principiul legitimității
- Principiul proporționalității
- Principiul acurateței și păstrării datelor
- Principiul siguranței



UN PRINCIPIU SUPLIMENTAR PRIVIND TRANSFERUL DATELOR

- Datele cu caracter personal nu ar trebui transferate în afara Zonei Economice Europene dacă țara în care se intenționează efectuarea transferului nu asigură o protecție adecvată acestor date;
- Directiva 95/46/CE prevede în Capitolul IV articolul 25 alineatul (1) ca "*transferul către o țară terță a datelor cu caracter personal care fac obiectul prelucrării sau sunt destinate prelucrării după transfer nu poate avea loc decât dacă, sub rezerva respectării dispozițiilor de drept intern [...], țara terță în cauză asigură un nivel de protecție adecvat,,.*
- CONFERĂ ȚĂRILE TERȚE UN NIVEL ADECVAT DE PROTECȚIE?

STATELE UNITE ȘI SISTEMUL SAFE HARBOUR



- "Safe Harbour" permite implementarea de către societățile interesate a unor măsuri de securitate asemănătoare cu cele prevăzute în Directivă
- Aplicabil numai întreprinderilor americane care subscriu la respectivul sistem, fără ca autoritățile publice din Statele Unite să fie ele însele supuse acestuia
- Sistemul a fost invalidat de Curtea Europeană de Justiție

CAZUL SCHREMS

DE CE ESTE IMPORTANT CAZUL SCHREMS?

- Domnul Maximilian Schrems, cetățean austriac, utilizează Facebook din anul 2008.
- Datele furnizate Facebook de domnul Schrems sunt transferate de la filiala irlandeză a Facebook pe servere situate pe teritoriul Statelor Unite, unde fac obiectul unei prelucrări.
- Domnul Schrems a depus o plângere la autoritatea irlandeză de protecție a datelor, considerând că dreptul și practicile din Statele Unite nu asigură o protecție suficientă a datelor transferate către această țară împotriva supravegherii de către autoritățile publice.
- Autoritatea irlandeză respinge plângerea iar Înalta Curte de Justiție a Irlandei este sesizată.
- 6 octombrie 2015: CJUE invalidează decizia Comisiei prin care se constată că Statele Unite ale Americii asigură un nivel adecvat de protecție.

CONSECINȚELE DECIZIEI CJUE

Societățile din România care transmit date cu caracter personal în Statele Unite ale Americii dar și societățile americane care prelucrează aceste date, bazându-se exclusiv pe certificarea Safe Harbour, vor trebui să implementeze soluții alternative pentru a-și putea continua activitatea în mod legal.

Alternative:

- Obținerea consimțământului ferm al persoanei vizate;
- Încheierea unui contract între societatea care transmite datele cu caracter personal și societatea care primește aceste date;
- Implementarea unor reguli corporative obligatorii (binding corporate rules, BCRs)

VIITORUL CADRU LEGAL

- Proiectul de Regulament al Parlamentului European și al Consiliului privind protecția persoanelor fizice față de prelucrarea datelor cu caracter personal și libera circulație a acestor date, va înlocui Directiva 95/46/CE
- Se așteaptă adoptarea acestuia în primăvara anului 2016
- Cum va schimba noul Regulament European abordarea în domeniul prelucrării datelor cu caracter personal?



ASPECTE NOTABILE

- Regulamentul va avea aplicabilitate directă
- Sancțiunile propuse pentru nerespectarea prevederilor Regulamentului pot ajunge până la 2% din cifra anuală de afaceri globală a unei societăți (de exemplu pentru societăți care prelucrează date fără un temei legal)
- Introducerea unor noi concepte, cum ar fi „*dreptul de a fi uitat*” (după cum acesta a fost recunoscut prin decizia CJUE în cazul Google Spania)
- Înființarea, cu titlu obligatoriu, a unei poziții – la nivel de societate sau de grup – intitulată „*data protection officer*” care va beneficia de o anumită siguranță crescută a locului de muncă.

CONCLUZII ȘI RECOMANDĂRI

- Societățile care prelucrează în mod frecvent date cu caracter personal și transferă aceste date către state din afara Spațiului Economic European ar trebui să ia în considerare efectuarea unui studiu de risc / audit intern, de exemplu prin identificarea principalelor fluxuri de date transferate de societate către terți sau în cadrul grupului și a temeiului legal în baza căruia datele sunt transferate, precum și evaluarea măsurilor de securitate implementate.
- În cazul în care datele personale ale angajaților sunt stocate în afara Uniunii Europene sau într-un sistem Cloud, mai ales în Statele Unite, societățile ar trebui să se asigure de existența unui temei legal pentru autorizarea transferului datelor precum și de existența unor măsuri de securitate adecvate la nivelul recipientului.

EXPERT



MULȚUMESC PENTRU ATENȚIA ACORDATĂ!



Alexandru Câmpean
Senior Associate
Wolf Theiss Wolf Theiss
Rechtsanwälte GmbH & Co KG

Bucharest Corporate Center
58-60 Gheorghe Polizu Street, 13th Floor
Bucharest, Romania
Tel: +40 21 308 81 00
E-mail: alexandru.campean@wolftheiss.com
www.wolftheiss.com

