# 25 mai 2018. Sunteți pregătiți?

TRANDAFIR&ASSOCIATES

Powerful Knowledge


Să conștientizăm GDPR

# Managementul procesului de conformare

- Auditul GDPR
- Situația datelor colectate înainte de 25 mai 2018
- Politica privind protecția datelor
- DPO
- Cerințele GDPR sunt aplicabile în privința datelor colectate în format electronic/digital, cât și a celor în format fizic
- Reevaluarea continuă/periodică
- Data protection by design and by default

TRANDAFIR&ASSOCIATES
Powerful Knowledge

# Auditul GDPR

**Scop**

- Data mapping
- Identificarea problemelor (raportat la cerințele GDPR) și a măsurilor de corecție
- Stabilirea instrumentelor necesar a fi utilizate pentru conformare

**Întrebări esențiale**

- Ce date cu caracter personal a colectat organizația de la persoanele vizate?
- Cum prelucrează organizația datele cu caracter personal colectate?
- A efectuat organizația schimburi de date cu caracter personal?
- A adoptat organizația vreo măsură de protecție pentru a asigura protecția datelor cu caracter personal?

# Date colectate anterior

- Identificați datele prelucrate fără consimțământul persoanelor vizate, și încercați să îl obțineți, iar dacă nu este posibil, doar atunci ștergeți acele date.
- Dacă ați colectat prea multe date, raportat la scopul colectării datelor, ștergeți definitiv ceea ce nu este absolut necesar.
- Dacă nu aveți măsuri de securitate implementate, auditul IT va identifica și va propune măsuri de securizare a datelor (de exemplu, criptarea lor).

Notă: Paragraful 171 din preambulul GDPR clarifică aplicarea tranzitorie a acestuia.

# Politica privind protecția datelor

- Datele de contact ale responsabilului cu protecția datelor cu caracter personal, atribuțiile sale, și felul în care acesta colaborează cu departamentele organizației
- Modalitatea în care organizația asigură respectarea drepturilor persoanelor vizate
- Felul în care persoanele vizate de prelucrare pot adresa în mod facil o plângere către organizație sau pot avea acces la datele proprii cu caracter personal
- Stabilirea unei o metode de retragere a consimțământului
- Cazurile în care datele pe care organizația le colectează și prelucrează pot fi trimise unei terțe părți

# DPO

Numirea unui DPO este obligatorie în următoarele cazuri (cf. art. 37 GDPR):

- când prelucrarea este efectuată de o autoritate publică sau un organism public
- când activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă
- când activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor categorii de date cu caracter personal privind condamnări penale și infracțiuni

# DPO - continuare

- Dacă DPO este salariat al organizației, trebuie să i se acorde posibilitatea de a acționa în mod independent; în principiu, calitatea de DPO este dificil de conciliat cu cerința independenței, cu atât mai mult cu cât specific raporturilor de muncă este subordonarea ierarhică.
- DPO nu se poate afla în conflict de interese.
- Indiferent de pregătirea sa profesională, DPO trebuie să aibă suport din partea unui avocat/jurist; doar avocatul/juristul are abilitatea de a da consultanță juridică, iar în caz de litigii, doar avocatul/juristul vă poate apăra, atât în relația cu ANSPDCP (e.g. asistență juridică pe parcursul controlului), cât și în cazul unui litigiu cu o persoană vizată.

# Digital vs. hard copy

- GDPR este pe deplin aplicabil în ceea ce privește colectarea, stocarea și arhivarea documentelor în format fizic
- Obligația de ținere a evidenței operațiunilor de prelucrare se aplică și informațiilor în format fizic, precum cereri, adrese, formulare, chestionare, etc.
- Organizațiile trebuie să aibă în vedere riscurile și provocările de ordin logistic: unde sunt ținute aceste informații, cine are acces la ele, cum se asigură păstrarea lor

Notă: Arhivarea documentelor este în sine o modalitate de prelucrare de date personale, care trebuie să respecte regulile GDPR.

# Reevaluarea continuă/periodică

- Conformarea este un proces continuu, justificat prin progresul tehnic
- GDPR nu stabilește cerințe minimale privind reevaluarea periodică (e.g. intervale, aspecte supuse reevaluării, etc.) – cf. art. 24 para. (1) GDPR
- Condițiile de reevaluare periodică trebuie detaliate în politica privind protecția datelor

# Data protection by design and by default

- Un principiu esențial, reglementat de art. 25 GDPR
- Orice obiect, aplicație IT sau tehnologie care folosește date personale va trebui să respecte cerințele GDPR
- Contractele care privesc asemenea „obiecte” trebuie să includă clauze privind respectarea GDPR (i.e. garanții, în sensul art. 1714 din codul civil cu privire la garanțiile pentru lipsa calităților convenite)
- Se pot implementa sisteme de certificare a conformității GDPR (cf. art. 42 GDPR), care să suplinească prevederile contractuale
- Orice entitate care prelucrează date personale trebuie să aplice „by default” acest principiu; cf. 25 para. (2): „*În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane*.”

# Cele mai frecvente greșeli

- Colectarea unui volum excesiv de date (se încalcă principiul minimizării prelucrării datelor)
- Păstrarea datelor personale pentru o durată excesivă (se încalcă principiul stocării limitate a datelor)
- Lipsa/încălcarea măsurilor de securitate fizică
- Prelucrarea fără consimțământ obținut în mod legal de la persoanele vizate
- Utilizarea interesului legitim ca bază a prelucrării conforme; acesta are caracter subsidiar; nu poate fi utilizat de către autoritățile publice (în cazul cărora, orice prelucrare trebuie să aibă o bază legală, potrivit principiului legalității)

# Relația operatorului cu autoritatea națională

- Răspunderea operatorului este reglementată de art. 5 para. (2) GDPR (principiul răspunderii operatorului) – operatorul are obligația legală de a demonstra că orice prelucrare de date personale este conformă cu principiile cuprinse în art. 5 para. (1) GDPR
- Măsurile de conformare dispuse de autoritate permit evitarea sancțiunilor

Notă: Conform para. (120) din preambulul GDPR, autoritățile naționale trebuie să dispună de resursele financiare și umane, spații de lucru și infrastructura necesară exercitării efective a competențelor stabilite prin GDPR, respectiv prin măsurile legislative naționale adoptate în marja de apreciere lăsată statelor membre prin GDPR.

# Relația operatorului cu persoana vizată

- Principiul răspunderii operatorului reglementat prin art. 5 para. (2) GDPR are impact practic asupra acțiunii judiciare
- Prejudiciul (material, moral)
- Aspecte practice (competența instanței, administrarea probelor, prescripția)
- Acțiunile colective
- Cf. para. 149 din preambulul GDPR, statele membre pot să stabilească și sancțiuni penale pentru încălcarea GDPR, cu posibilitatea confiscării profiturilor/beneficiilor obținute din activitățile de prelucrare neconforme

# Relația operatorului cu alte autorități naționale

- Colectarea și procesarea de date personale în baza legislației specifice, neadaptate/nerevizuite
- Transferul de date personale către autoritățile publice
- Răspunderea pentru breșe de securitate

Notă: A se avea în vedere Comunicarea Comisiei către Parlamentul European și către Consiliu COM (2018) 43 din data de 24.01.2018, care evaluează stadiul adaptării legislației interne de către statele membre la data de referință anterior indicată.

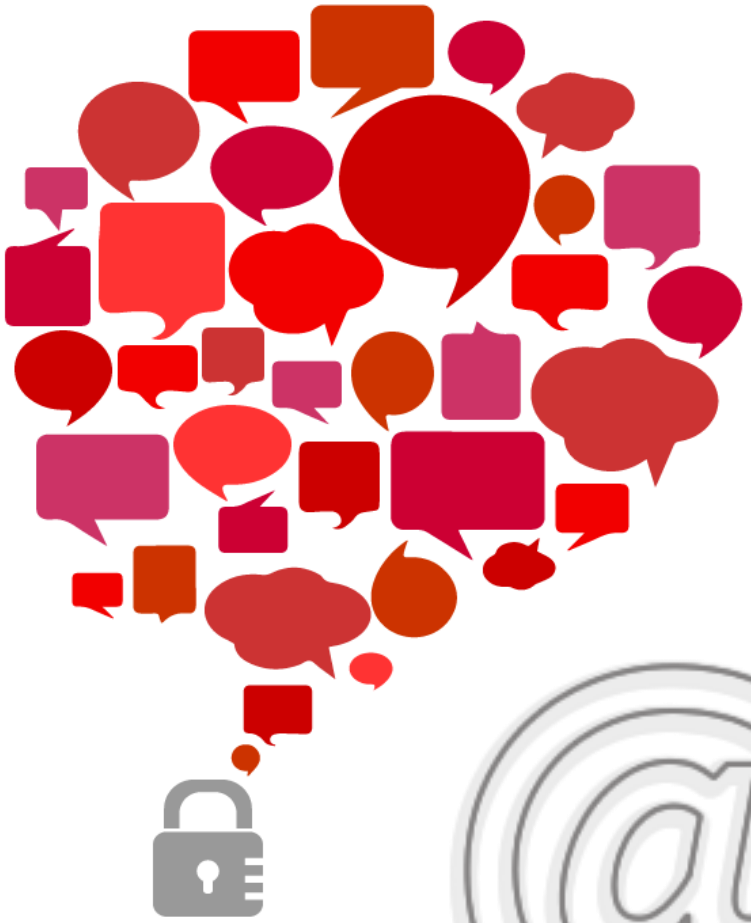
TRANDAFIR&ASSOCIATES
Powerful Knowledge

# Studiu de caz – impactul GDPR asupra turismului

- Cum se colectează date personale?
- Industria turismului colectează cantități impresionante de date personale.
- Oare toate tipurile de informații solicitate sunt cu adevărat necesare?
- Ce se întâmplă apoi cu aceste date?
- În cazul utilizării aplicațiilor de mobil, acestea trebuie să respecte aceleași cerințe ca și pagina web. Nu uitați, peste 95% din email-uri se citesc acum pe mobil.
- Dacă un client nu și-a dat acordul pentru publicitate ulterioară, acesta nu poate fi contactat, în principiu.

TRANDAFIR&ASSOCIATES

Powerful Knowledge



(+4) 031 438 22 54

office@trandafir.biz