MOORE STEPHENS

Congress CAFR

Impactul Regulamentului de Protectie a Datelor cu Caracter Personal in Misiunea de Audit

November 2017

Mai multă muncă de conformitate

- Standarde noi: IFRS 9, IFRS 15, BASEL IV
- Reguli noi: GDPR
- Tehnici: RPO, Data Analytics, Big Data

GDPR Schimbări esențiale

Din perspectiva UE, GDPR înlocuiește Directiva 95/46 / CE privind protecția datelor și, deși există o mulțime de asemănări şi o serie de principii rămân neschimbate, obiectivul principal al GDPR este de a oferi cetățenilor deţinerea unui control asupra datelor lor personale, simplificând totodată mediul de reglementare pentru companiile internaționale. GDPR reprezintă, de asemenea, un uriaș pas înainte în optările Comisiei Europene pentru o "piață unică digitală".
Deși data de punere în aplicare nu va fi mai degrabă decât la 25 mai 2018, modificările principale ale GDPR detaliate în paginile următoare necesită o atenție imediată, deoarece va dura ceva timp pentru o pregătire prealabilă.

- Emis: 14 April 2016
- Aplicabilitate: 25 May 2018
- Aplicarea legislaţiei locale nu este necesară

Domeniul de aplicare teritorial sporit

Ca urmare a aprobării GDPR, există acum o jurisdicție extinsă reglementată de acest regulament, care este aplicabilă tuturor societăților care prelucrează date cu caracter personal ale persoanelor vizate care au reședința în Uniune, indiferent de locația societății.

Aplicabilitatea teritorială anterioară a fost ambiguă, cu toate acestea GDPR stipulează foarte clar – procesarea datelor cu caracter personal se va efectua de către controlori sau procesatori din UE, indiferent dacă procesarea datelor are loc în UE sau nu. GDPR va aplica, de asemenea, un controlor sau un procesator, care nu este stabilit în UE pentru procesarea datele cu caracter personal ale persoanelor vizate din UE, în scopul de a include oferirea de bunuri sau servicii cetățenilor UE și deasemenea în scopul monitorizării comportamentelor în cadrul UE.

Întreprinderile din afara UE care procesează datele cetățenilor UE vor trebui, de asemenea, să numească un reprezentant în UE.

Sancşiuni

Orice organizație care încalcă GDPR poate fi amendată cu până la 4% din cifra totală de afaceri sau 20 milioane EUR – fiecare dintre aceste sancţiuni fiind mai mare în cazurile încălcărilor grave ale regulamentului, de ex. dacă nu există un consimțământul relevant în vigoare.

Există, de asemenea, o abordare punctată a sancțiunilor aplicate pentru încălcări mai puțin grave, în aceste cazuri o întreprindere ar putea fi amendată cu până la 2% din cifra totală de afaceri sau 10 milioane USD – fiecare dintre aceste sancţiuni fiind mai mare, de ex. pentru lipsa registrelor de evidenţă necesare sau pentru a nu raporta o încălcare a autorității de supraveghere și a persoanelor vizate.

Trebuie remarcat faptul că aceste reguli se aplică atât controlorilor de date, cât și operatorilor.

GDPR Schimbări esențiale

Notificarea unei încălcări

Notificarea încălcărilor devine obligatorie în toate statele membre atunci când, ca urmare a unei încălcări, există riscul ca drepturile și libertățile persoanelor să devină compromise. În conformitate cu GDPR, notificarea trebuie raportată în termen de 72 de ore de la identificarea încălcării.

De asemenea, procesatorii de date trebuie să-și notifice clienții, controlorii "fără întârzieri nejustificate" după identificarea oricărei încălcări.

Ttransferabilitatea datelor

GDPR introduce transferabilitatea datelor - dreptul unui subiect de date de a primi datele personale care îi vizează, pe care le-a furnizat anterior într-un format obișnuit și care au fost prelucrate de către mașină și au dreptul de a re-transmite aceste date unui alt controlor.

Dreptul la acces

Drepturile persoanelor vizate au fost consolidate într-o oarecare măsură în cadrul GDPR. Persoana vizată are acum dreptul de a obține de la operatorul de date confirmarea unde și cum sunt procesate datele cu caracter personal și în ce scop.

Ca urmare a acestei solicitări, operatorul de date trebuie să furnizeze gratuit într-un format electronic o copie a datelor personale deținute, consolidând în continuare cerințele de transparență a datelor.

GDPR Schimbări esențiale

We provide support strategies and solutions to navigate the challenging environment.

Dreptul de a fi uitat

În conformitate cu GDPR, persoana vizată are acum dreptul de a fi uitată, cee ace oferă dreptul persoanei vizate de a-i fi șterse datele personale de către operatorul de date, de a înceta diseminarea în continuare a datelor și, eventual, de a opri prelucrarea datelor de către terți.

Condițiile de ștergere includ datele deținute care nu mai sunt relevante pentru scopurile inițiale pentru care au fost colectate şi procesate, sau în cazul în care un subiect își retrage consimțământul pentru utilizarea datelor.

Trebuie remarcat faptul că operatorii de date ar trebui să compare (contrapună) drepturile subiecților de date cu "interesul public pentru disponibilitatea datelor" atunci când iau în considerare astfel de solicitări.

Confidenţialitate prin design

Acum, o cerință în cadrul GDPR, confidențialitatea prin design, solicită includerea protecției datelor mai degrabă de la debutul proiectării sistemelor, fără solicitări adăugătoare.

Acest lucru va asigura faptul că operatorul respectă cerințele prezentului regulament și protejează drepturile persoanelor vizate.

Pentru a face acest lucru, controlorii trebuie să dețină și să proceseze numai datele absolut necesare pentru îndeplinirea sarcinilor sale, precum și să limiteze accesul la datele cu caracter personal celor care trebuie să efectueze procesarea.

GDPR Schimbări esențiale

We provide support strategies and solutions to navigate the challenging environment.

Ofiţeri pe Protecţia datelor (DPO)

În prezent, controlorii sunt obligați să notifice autoritățile locale pentru protecția datelor (DPA) în ceea ce privește activitățile de prelucrare a datelor. Acest lucru se dovedeşte a fi unul problematic pentru organizațiile multinaționale , iar în cadrul GDPR nu mai este necesar ca organizațiile să notifice individual fiecare DPA locală despre activităților lor.

În schimb, vor exista registre interne de păstrare a înregistrărilor, iar denumirea DPO va deveni obligatorie numai pentru controlorii și procesorii activitățile principale ale cărora constau în operațiuni de prelucrare, care necesită o monitorizare sistematică și sistemică, a persoanelor vizate la scară largă sau a unor categorii speciale de date, sau date privind condamnările penale și infracțiunile.

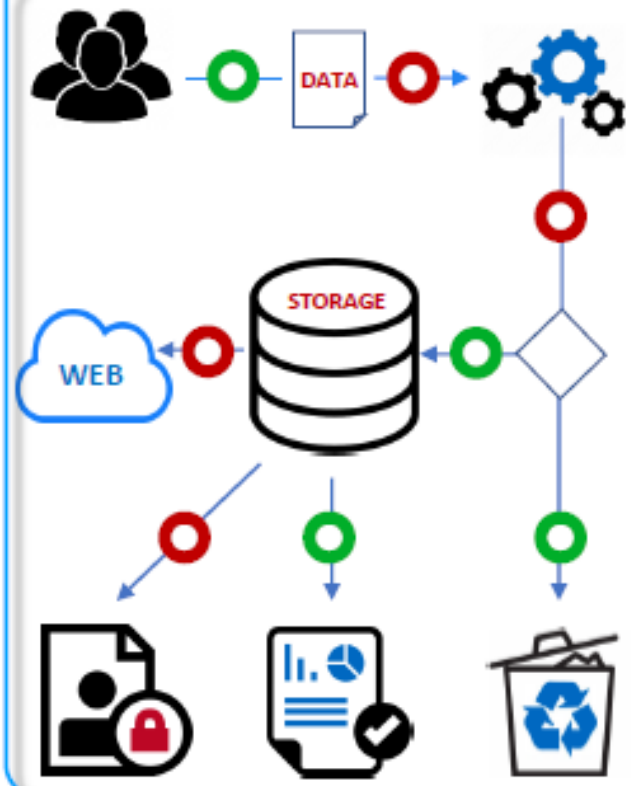
DPO:
trebuie să fie numiți în baza calităților lor profesionale și, în special, în baza cunoștințelor de experţi în domeniul legislaţiei şi practicilor privind protecţiei datelor;
poate fi un membru al personalului sau un furnizor extern de servicii;
datele de contact trebuie furnizate DPA-ului relevant pentru asigurarea legăturii în cadrul organizației;
trebuie să fie asigurat cu resurse adecvate pentru a-și îndeplini sarcinile și a-și păstra cunoștințele de expert în specialitate;
trebuie să raporteze direct la cel mai înalt nivel de conducere;
nu trebuie să îndeplinească alte sarcini care ar putea duce la un conflict de interese.

GDPR Implementation

1 Readiness assessment

- Resources
- People
- Data
- Processes

2 Gap analysis



3 GDPR implementation

- Data flow mapping
- Update organizational structures, policies and procedures
- Changes in IT systems
- Staff training
- Regular assessments and updates

AS IS → **TO BE**

Questions or comments?

Va multumesc!