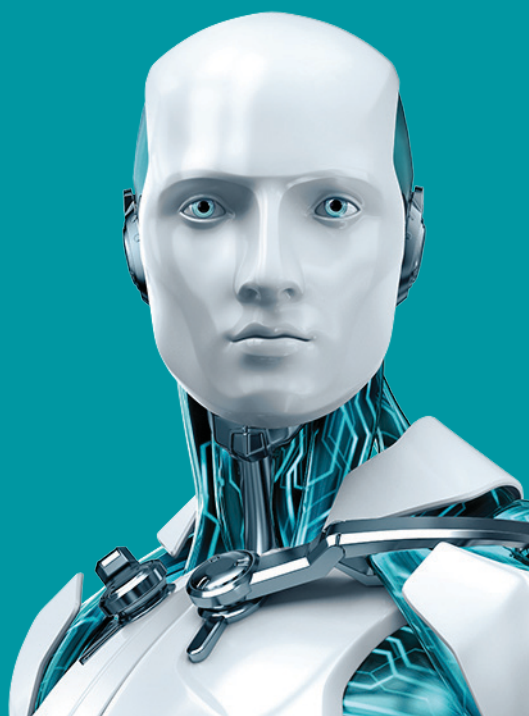
GDPR

ADUCE GDPR-UL VEȘTI BUNE SAU PROASTE PENTRU AFACERI?

Bazat pe:
“Un ghid concis al principalelor dispoziții ale Regulamentului General privind Protecția Datelor (GDPR) “de Kemp Jones Solicitors LLP



ENJOY SAFER TECHNOLOGY™

Cuprins

REZUMAT

În ultimii ani au fost înregistrate progrese majore în tehnologia informației și schimbări fundamentale ale modului în care persoanele și organizațiile comunică și împărtășesc informații. Cu toate acestea, în timp ce aceste evoluții au condus la o utilizare mai frecventă a datelor, tendința nu a fost reflectată în mod egal în toate codurile juridice ale statelor membre ale UE.

Pentru a realiza o armonizare în acest sens, a fost adoptată o nouă lege unică ce vizează protecția datelor, Regulamentul General privind Protecția Datelor (GDPR), care va intra în vigoare pe 25 mai 2018. Modificările aduse vor avea implicații asupra companiilor de toate dimensiunile care procesează datele personale ale cetățenilor europeni, indiferent dacă sunt sau nu în UE.

Unele concepte de bază existente în cadrul actualului regim UE de protecție a datelor (Directiva privind Protecția Datelor sau DPD introdusă în 1995) vor rămâne în general similare, precum conceptul de date cu caracter personal, controlorii de date și procesatorii de date. Cu toate acestea, vor intra în vigoare **multe noi concepte și abordări**, ceea ce ar putea crea dificultăți de conformitate pentru companii.

Printre modificările semnificative se numără:
- Domeniul teritorial extins, incluzând companiile din UE, precum și cele din afara UE
- Amenzi mai mari și o gamă mai largă de competențe pentru Autoritățile Naționale de Protecție a Datelor (ANPD)
- Reguli mai stricte pentru dobândirea și retragerea consimțământului unei persoane
- Reguli mai stricte de notificare a breșelor

GDPR extinde, de asemenea, drepturile persoanelor, prin acordarea acestora:
- A dreptului de a se opune la profilare
- A dreptului de a obține o copie a datelor colectate
- A dreptului de a fi uitat

Cu toate acestea, GDPR reprezintă și o veste bună pentru companiile care lucrează cu date. Acesta va elimina variațiile excesive la nivel național ale obligațiilor de respectare a protecției datelor și le va înlocui cu un set comun de reguli, reducând în principal sarcina pentru companiile multinaționale.

Un alt avantaj este trecerea la conceptul de "ghișeu unic", care va permite companiilor să se adreseze unei singure autorități de protecție a datelor.

Acest ghid oferă o descriere mai detaliată a elementelor cheie menționate mai sus, precum și a altor câteva modificări aduse de GDPR.

GDPR: UN SET MAI COERENT DE REGULI DE PROTECȚIE A DATELOR

GDPR introduce un cadru juridic unic, care se aplică tuturor statelor membre ale UE, ceea ce înseamnă că întreprinderile se vor confrunta cu un set mai consistent de obligații de respectare a protecției datelor de la un stat membru UE la altul.

Dar GDPR nu face referire numai la companii sau la entități care lucrează cu date cu caracter personal în cadrul UE. Multe companii sau organizații din afara UE care nu au fost obligate să respecte fostul regulament (Directiva privind Protecția Datelor sau DPD) vor fi nevoite să respecte noile norme.

Subiectul datelor - *persoană fizică ale cărei date cu caracter personal sunt prelucrate de un operator sau de un procesator.*

Din motive de claritate, pe tot parcursul acestui raport, termenul va fi denumit și **client sau angajat.**

O companie este supusă regulamentului, dacă:
- oferă bunuri sau servicii persoanelor vizate din UE indiferent dacă acestea sunt plătite
- monitorizează comportamentul subiecților în cadrul UE

În ciuda introducerii unui cadru legislativ mai rațional, GDPR poate determina schimbări semnificative pentru multe companii, ceea ce necesită un timp îndelungat de procesare.

Autoritățile Naționale de Protecție a Datelor vor câștiga mai multă putere

În prezent, amenzile în temeiul legislației naționale variază și sunt relativ scăzute, ajungând la sute de mii în unele țări. GDPR va majora în mod semnificativ amenzile maxime, făcând neconformitatea o problemă de risc foarte mare. Sancțiunile trebuie împărțite în două grupe.

1. **Până la 2% din cifra de afaceri anuală globală a anului financiar precedent** sau **10 milioane de euro** (valoarea mai mare dintre acestea) pentru încălcările privind păstrarea înregistrărilor interne, contractele de procesare a datelor, securitatea datelor și notificarea breșelor, ofițerii de protecție a datelor și protecția datelor prin configurare sau implicită
2. **Până la 4% din cifra de afaceri anuală globală a anului financiar precedent** sau **20 de milioane de euro** (valoarea mai mare dintre acestea) pentru încălcările referitoare la principiile privind protecția datelor, la condițiile pentru consimțământ, la drepturile persoanelor vizate și la transferurile internaționale de date.

Competențele Autorităților Naționale pentru Protecția Datelor (ANPD) vor crește, de asemenea, pentru a le permite:
- Impunerea amenzilor menționate mai sus
- Efectuarea de audituri
- Solicitarea companiilor să furnizeze informații
- Obținerea accesului la sediul companiei

Procesator de date - *entitatea care procesează datele în numele controlorului de date.*

*Din motive de claritate, pe tot parcursul acestui document, se va menționa termenul de "***companie de procesare.***"*

Obținerea consimțământului devine mai dificilă

Înainte de GDPR, **consimțământul obișnuit** era necesar pentru datele cu caracter personal ce nu erau considerate sensibile, iar **consimțământul explicit** pentru datele personale sensibile.

Din data de 25 mai 2018, subiecții datelor trebuie să dea consimțământul în toate cazurile *"printr-o acțiune afirmativă clară ce stabilește o indicație individuală, specifică, informată și lipsită de ambiguitate a acordului persoanei față de prelucrarea datelor sale cu caracter personal, cum ar fi printr-o declarație scrisă."*

Companiile își vor asuma sarcina probei conform căreia clienții sau angajații și-au dat acordul pentru prelucrarea datelor lor și că acesta a fost obținut într-un mod valid. În cazul în care prelucrarea are scopuri multiple, consimțământul este necesar pentru fiecare dintre acestea separat.

În plus, utilizatorii finali, clienții și angajații trebuie să își poată retrage consimțământul în orice moment, având în vedere că aceste proceduri vor fi la fel de simple precum acordarea consimțământului.
Mai mult decât atât, companiile nu mai pot solicita consimțământul în schimbul serviciilor lor sau "a executării contractului" și nu mai pot folosi date inutile pentru aceste activități.

Abordarea bazată pe riscuri privind conformitatea

În conformitate cu noile norme GDPR, întreprinderile vor fi responsabile pentru evaluarea gradului de risc cu privire la activitatea de prelucrare pentru persoanele vizate - cum ar fi utilizatorii finali, clienții sau angajații

Acest lucru poate fiinterpretat în mai multe dispoziții, cum ar fi noul principiu al asumării și cerința ca administratorii de date să mențină documentația, confidențialitatea în mod deliberat și implicit, evaluările impactului asupra confidențialității, cerințele privind securitatea datelor și numirea unui responsabil cu protecția datelor.

Activitățile de prelucrare cu risc redus se pot confrunta cu o conformitate a sarcinii reduse.

Controlor de date - *entitatea care determină scopurile, condițiile și mijloacele de prelucrare a datelor cu caracter personal.*

Din motive de claritate, pe tot parcursul acestui document se va menționa termenul de **companie de control sau de companie aflată în control**.

"Ghișeul unic"

Pentru companiile multinaționale, prezente pe mai multe piețe ale UE, GDPR va reprezenta o schimbare substanțială în comunicarea cu autoritățile de protecție a datelor. Acesta permite companiilor să comunice și, în mod predominant, să se adreseze unei singure autorități (ANPD).

Aceasta este, de asemenea, descrisă ca o "autoritate de supraveghere principală", responsabilă în mod obișnuit de organizarea principală a afacerii în cadrul UE.

Conducerea ANPD va fi responsabilă pentru toate reglementările activităților de prelucrare transfrontaliere efectuate de respectiva companie de control sau prelucrare. De asemenea, trebuie să colaboreze cu toate celelalte ANPD-uri în cauză, deoarece toate au un cuvânt de spus în deciziile de executare referitoare la activitățile de prelucrare transfrontaliere.

Dacă aceste autorități nu pot ajunge la un acord asupra unei decizii, problema este adresată **Autorității Europene pentru Protecția Datelor (AEPD)**. Acesta are o serie de competențe pentru a asigura aplicarea consecventă a GDPR în întreaga Uniune - inclusiv autoritatea de a lua decizia finală în cazurile de executare. Cazurile locale vor continua să fie tratate de către ANPD pentru jurisdicția locală.

NOI OBLIGAȚII ALE COMPANIILOR ÎN CADRUL GDPR

Confidențialitate prin concepție sau implicită

În special, GDPR va impune întreprinderilor să implementeze măsuri tehnice și organizaționale pentru a se asigura că sunt îndeplinite cerințele GDPR - "confidențialitatea prin concepție", precum și "confidențialitatea în mod implicit".

Companiile trebuie să țină seama de cerințele privind protecția datelor de la faza incipentă a oricărei noi tehnologii, a produselor sau serviciilor ce implică prelucrarea datelor cu caracter personal (în mod deliberat) și aplicarea măsurilor adecvate pentru prelucrarea datelor (confidențialitatea implicită).

GDPR numește mai multe măsuri care pot ajuta companiile să atingă aceste obiective - menționând minimizarea procesării datelor cu caracter personal, criptarea sau pseudonimizarea datelor, transparența în ceea ce privește funcțiile și prelucrarea lor, permițând subiecților să monitorizeze modul în care sunt gestionate datele. Aceste măsuri trebuie, de asemenea, să fie actualizate.

Evaluări obligatorii ale impactului asupra confidențialității

Dacă este posibil ca tehnologiile recent dezvoltate să ducă la un risc ridicat pentru utilizatorii finali, clienți sau angajați, companiile vor fi obligate să efectueze evaluări de impact privind protecția datelor (IPD) înainte de a efectua orice prelucrare.

În mod special, evaluările vor fi necesare pentru:

- O evaluare sistematică și extinsă a aspectelor personale prin prelucrare automată, ce creează baza deciziilor care produc efecte juridice asupra persoanelor vizate sau le afectează în mod semnificativ. În această categorie este inclusă crearea de profiluri.
- Prelucrarea categoriilor speciale de date cu caracter personal sau a datelor referitoare la condamnările penale și infracțiunile la scară largă.
- O monitorizare sistematică a unei zone accesibile publicului la scară largă
- Alte tipuri de operațiuni de prelucrare care necesită o evaluare, publicată de ANPD.

Companiile de control pot efectua o evaluare unică pentru a aborda un set de operațiuni de prelucrare similare ce prezintă riscuri asemănătoare.

Atunci când o evaluare indică faptul că prelucrarea ar avea ca rezultat un risc ridicat pentru persoanele fizice, înainte de orice procesare, compania trebuie să se consulte cu ANPD.

Pictogramele standardizate folosite pentru a indica anumite caracteristici importante ale activităților relevante de prelucrare a datelor într-un format simplificat pot fi prescrise prin acte delegate.

Fără înregistrări

În cazul unei înregistrări la o autoritate, companiile de control vor trebui să păstreze o documentație detaliată care să înregistreze activitățile lor de prelucrare.

În mod similar, companiile de prelucrare trebuie să țină evidența categoriilor de activități de prelucrare pe care le efectuează în numele unei societăți aflate în proces de controlare. GDPR specifică informațiile pe care fiecare înregistrare trebuie să le conțină în fiecare dintre instanțele menționate mai sus.

Acest lucru nu se aplică întreprinderilor care angajează mai puțin de 250 de persoane, cu excepția cazului în care: 1.) este posibil ca prelucrarea să aibă ca rezultat un risc ridicat pentru persoane fizice; 2.) prelucrarea nu este ocazională sau 3.) prelucrarea include date sensibile cu caracter personal.

Numai în anumite circumstanțe, întreprinderile de control sau de prelucrare pot fi obligate să numească un responsabil cu protecția datelor, ce are cunoștințe de specialitate în domeniul protecției datelor. Un angajat aflat într-o astfel de poziție poate avea statut de angajat protejat.

Noi obligații pentru cei care prelucrează date

Întrucât, în conformitate cu reglementările anterioare, societățile de prelucrare nu erau, în general, supuse unor amenzi sau altor sancțiuni, în urma aplicării noului regulament, GDPR va schimba acest lucru. Procesatorii pot fi obligați să plătească amenzi de până la 4% din cifra anuală globală de afaceri de din anul financiar precedent sau 20 de milioane de euro, oricare dintre valori este mai mare.

Creșterea obligațiilor de conformitate va duce probabil la o creștere a costului serviciilor de prelucrare a datelor. Această creștere poate, de asemenea, să facă dificilă negocierea acordurilor de prelucrare a datelor, deoarece operatorii vor avea un interes mai mare pentru a se asigura că scopul instrucțiunilor operatorului este unul clar.

Acest lucru poate conduce, de asemenea, la o revizuire a acordurilor existente, pentru a se asigura că societățile de prelucrare și-au îndeplinit propriile obligații în temeiul GDPR. Prin urmare, societățile aflate în proces de controlare trebuie să identifice acordurile care ar putea necesita o revizuire și să le modifice, dacă este necesar.

Reguli stricte de notificare a încălcării datelor

GDPR solicită întreprinderilor să notifice NDPA cu privire la toate breșele de date, fără întârzieri nejustificate, în termen de maximum 72 de ore, cu excepția cazului în care este puțin probabil ca încălcarea datelor să ducă la un risc pentru persoanele vizate individuale. Dacă acest lucru nu este posibil, compania va trebui să justifice întârzierea către ANPD printr-o "justificare argumentată"
În cazurile în care breșa este susceptibilă să genereze un risc ridicat pentru persoanele fizice, GDPR cere companiilor să informeze persoanele vizate, "fără întârzieri nejustificate", cu excepția cazului în care se aplică o excepție. Procesatorii de date trebuie să notifice controlorul de date.

Pe baza acestor noi reguli, companiile vor fi nevoite să creeze un plan de răspuns la breșele de date, care să le permită să reacționeze prompt în cazul unei astfel de breșe. Acest lucru va necesita, de asemenea, desemnarea anumitor roluri și responsabilități în cadrul companiei, precum și formarea angajaților și pregătirea șabloanelor de notificare.

Respectarea noilor reguli GDPR pentru raportarea breșelor va implica o sarcină administrativă semnificativă, ce poate duce la creșterea costurilor pentru companii.

Criptarea - *este procesul de codificare a informațiilor într-un mod care împiedică părțile neautorizate să le poată citi.*

Criptare

Comunicarea breșelor de date cu privire la persoanele vizate nu va fi necesară dacă operatorul a implementat măsuri de protecție adecvate. Acest lucru se aplică în mod specific mijloacelor care fac ca datele personale să fie incomprehensibile pentru orice persoană care nu este autorizată să le acceseze.

Criptarea îndeplinește acest obiectiv, fiind denumită în mod explicit de către GDPR drept una dintre cele mai potrivite măsuri tehnice și organizaționale pe care întreprinderile trebuie să le pună în aplicare pentru a asigura un nivel de securitate adecvat riscului.

Reguli corporatiste obligatorii (RCO)

GDPR introduce o gamă puțin mai largă de mecanisme pentru transferul datelor cu caracter personal în afara Spațiului Economic European (SEE).

Aceasta recunoaște în mod oficial regulile corporative obligatorii (RCO) - acorduri utilizate în acest scop în trecut - ca un mecanism legal de transfer de date (în timp ce variantele anterioare GDPR nu o făceau).

În conformitate cu noul regulament, conform acestor reguli va fi solicitată în continuare aprobarea ANPD, însă procesul ar trebui să devină mai puțin împovărător față de cum este în sistemul actual. RCO-urile sunt disponibile atât companiilor de control cât și celor de prelucrare.

Întreprinderile ar trebui să-și revizuiască procedurile și baza juridică în ceea ce privește transferul de date cu caracter personal în afara SEE și să țină acest lucru sub control, în special din moment ce validitatea mecanismelor de transfer continuă să fie examinată de Curtea de Justiție a Uniunii Europene pe fondul cazurilor în curs.

Amenzile pentru încălcarea restricțiilor privind transferul de date în cadrul GDPR se încadrează în categoria superioară pentru nerespectarea cerințelor

NOI DREPTURI PENTRU SUBIECȚII DATELOR

În general, drepturile clienților sau ale angajaților (respectiv persoanele vizate) sunt extinse în cadrul GDPR. Lista noilor drepturi individuale include:

Dreptul de a fi uitat

Persoanele fizice vor avea dreptul să solicite companiilor ștergerea datelor cu caracter personal în anumite circumstanțe. De exemplu, acest lucru este posibil în cazul în care informațiile nu mai sunt necesare pentru scopul în care au fost colectate sau persoana vizată își retrage consimțământul.

Ca urmare a deciziei instanței, este posibil ca multe companii să facă deja acest lucru. Cu toate acestea, nu se știe exact cum va funcționa în practică, iar întreprinderile ar trebui să ia în considerare modurile în care vor aplica în mod adecvat acest drept, deoarece ștergerea datelor cu caracter personal nu este întotdeauna simplă.

Profilarea - *este definită pe larg și include majoritatea formelor de urmărire online și de publicitate comportamentală, ceea ce face mai dificilă utilizarea de către companii a datelor pentru aceste activități. Procesul profilare trebuie să fie dezvăluit persoanei vizate și este necesară o evaluare de tip IPD.*

Dreptul de a se opune profilării

În anumite circumstanțe, persoanele fizice vor avea dreptul să se opună prelucrării datelor lor personale (în acest sens, se încadrează profilarea).

Pentru companiile care utilizează profilarea numai în cazuri rare, poate fi mai ușor să se încheie astfel de activități, decât să se respecte normele GDPR. Companiile care se angajează în mod regulat să elaboreze profiluri trebuie să aibă în vedere modalitatea cea mai bună de a pune în aplicare mecanismele adecvate de consimțământ.

Asociația Europeană pentru Protecția Datelor va urma să furnizeze orientări suplimentare privind profilarea.

Dreptul la portabilitatea datelor

Persoanele vizate au un nou drept de a obține o copie a datelor lor personale de la societatea care deține controlul într-un format utilizat în mod obișnuit și digital. Aceștia vor avea, de asemenea, dreptul de a transmite aceste date unui alt controlor - de exemplu, un alt furnizor de servicii online.

În exercitarea acestui drept, persoanele vizate pot solicita ca informațiile să fie transmise direct de la un controlor la altul, dacă este fezabil din punct de vedere tehnic.

Întreprinderile care procesează cantități mari de date cu caracter personal (cum ar fi companiile din domeniul rețelelor de socializare, companiile de asigurări sau băncile) ar trebui să ia în considerare modul în care fac aceste drepturi accesibile.

În timp ce companiile online noi pot interpreta acest lucru ca o modalitate de îmbunătățire a concurenței, furnizorii stabiliți o vor vedea probabil în termeni mai puțin avantajoși.

Cererile de acces la datele stocate

Compania trebuie să răspundă în termen de o lună de la data primirii cererii și să furnizeze mai multe informații decât era cerut de regulamentele anterioare GDPR-ului.

CUM POATE AJUTA ESET?

După cum a fost menționat deja, GDPR nu introduce doar reguli mai stricte pentru protecția datelor personale aparținând persoanelor fizice, ci evidențiază și măsurile considerate potrivite pentru locul de muncă - numind criptarea drept una dintre ele.

În general, printre avantajele principale ale tehnologiei de criptare se numără puterea acesteia - datorită algoritmilor puternici și a creșterii lungimii cheilor (biți) - disponibilitatea largă și costurile relativ scăzute de implementare, tehnologie adoptată chiar de unele autorități naționale.

Spre exemplu, DESlock Encryption by ESET, oferă mai mult decât elementele de bază. De asemenea, oferă clienților business o soluție ușor de implementat, ușor de utilizat chiar și pentru utilizatorii atehnici și care permite gestionarea la distanță a cheilor, setărilor și politica de securitate. De asemenea, permite utilizatorilor să cripteze în condiții de siguranță hard disk-urile, unitățile detașabile, fișierele și e-mailurile.

În plus, criptarea DESlock permite companiilor să îndeplinească obligațiile impuse de GDPR cu privire la securitatea datelor prin aplicarea cu ușurință a politicilor de criptare, menținând în același timp productivitatea ridicată. În afară de toate acestea, DESlock Encryption by ESET rezolvă una dintre cele mai mari provocări privind aplicabilitatea: cum pot utilizatorii să împartă informații criptate?

Parolele comune reprezintă un potențial risc de securitate, iar criptarea cu chei publice poate cauza probleme , în special în echipe mai mari, cu o rată mare de schimbare a personalului. Cheile de criptare administrate la nivel central, evită aceste obstacole, reflectând o cale mai naturală - asemănătoare cu utilizarea cheilor fizice pentru a bloca mașini sau case.

Mai multe informații legate de GDPR și de DESlock Encryption pot figăsite pe pagina dedicată GDPR de la ESET.

CONCLUZIE: ARGUMENTE PRO ȘI CONTRA PENTRU GDPR

GDPR are potențialul de a introduce schimbări pozitive pentru multe companii. Acesta este destinat să sporească unificarea legislațiilor naționale privind protecția datelor în UE, abordând, în același timp, noile evoluții tehnologice. GDPR va fi direct aplicabil în întreaga Uniune Europeană, fără a fi nevoie de implementare la nivel național, în acest fel întreprinderile se vor confrunta cu mai puține variații naționale în ceea ce privește normele de protecție a datelor.

De asemenea, companiile pot beneficia de abordarea "ghișeului unic", care le va permite să se adreseze în primul rând unei singure autorități. Cu toate acestea, există încă zone în care diferențele materiale vor continua să existe, de la un stat membru la altul, afectând cerințele de respectare a protecției datelor (inclusiv aspectele legate de securitatea națională, jurnalismul, libertatea de exprimare, dreptul muncii, legile privind confidențialitatea profesională și legile privind interceptarea comunicațiilor).

Pe de altă parte, este posibil ca GDPR să necesite modificări la nivel de organizație pentru multe companii din UE, deoarece va trebui să se asigure că datele cu caracter personal sunt prelucrate în conformitate cu noile cerințe stabilite.

Astfel de modificări pot include sisteme de reproiectare care prelucrează date cu caracter personal, renegocierea contractelor cu procesatori terți de date și restructurarea acordurilor transfrontaliere în ceea ce privește transferul de date. De asemenea, poate duce la adaptarea unor măsuri organizaționale și tehnice, cum ar fi criptarea.

Companiile ar trebui, prin urmare, să considere că aceste schimbări pot necesita o perioadă semnificativă de timp pentru punerea în aplicare și planificarea în viitor. Nerespectarea acestor prevederi ar putea însemna că întreprinderile au parte de noi cerințe de implementare, fără a fi fost rezervate în prealabil resursele adecvate, necesare pentru a se conforma.

Aflați mai multe detalii:
encryption.eset.com/ro

eset
ENJOY SAFER
TECHNOLOGY™