ROMÂNIA
JUDEŢUL BRAŞOV
COMUNA HÂRSENI
Str. Principală, nr. 175, Tel. : (004) 0268/247800 ; fax : 0268/247832
cod fiscal 4384591, e-mail: comunaharseni@yahoo.com

ROMÂNIA

Nr. 2833 / 23.05.2018

ROMÂNIA JUD. BRAŞOV COMUNA HÂRSENI

APROB , PRIMAR

Oltean Mihai

REGULAMENT

Ghid punere in practica Regulament GDPR 679/2016

Acest ghid ofera o explicație pe înțelesul tuturor a ceea ce presupune noul regulament de protecție al datelor personale și care sunt măsurile care trebuie luate pentru o Primărie pentru a fi în conformitate cu GDPR.

În primul rând, trebuie inteles faptul ca primăria este operator de date cu caracter personal.

Orice agent economic care colectează și procesează date cu caracter personal este operator de date, deci trebuie să se conformeze GDPR până la 25 mai 2018. Acest regulament va înlocui de la această dată Legea 677/2001 privind protecția datelor cu caracter personal.

GDPR – Global Data Protection Regulation – este un regulament adoptat la nivel de UE a cărui obiectiv general este de a crește nivelul de protecție al datelor cu caracter personal.

În acest sens GDPR:

- Impune adoptarea unui set de măsuri cu caracter OBLIGATORIU.

- Recomandă foarte ferm o serie de principii de conduită și măsuri de protejare a datelor a căror respectare trebuie să le putem dovedi în cazul unui control.
- **Stabilește niște sancțiuni extrem de severe** pentru a se asigura luarea în serios a protecției datelor de către operatori.

Nr	Măsuri de adoptat	Caracter
1	Desemnarea unui ofițer de protecția datelor – DPO – până la 25 mai 2018.	Obligatoriu
2	Raportarea scurgerile de date către autorități în maxim 72 de ore de la identificare.	Obligatoriu
3	Inventarierea în scris echipamentele din cadrul Instituției.	Recomandare fermă
4	Definirea temeiului legal de colectare a datelor.	Recomandare fermă
5	Evaluarea riscurilor de scurgere de date.	Recomandare fermă
6	Formularea în scris un set de proceduri tehnice și de conduită pentru prelucrarea datelor.	Recomandare fermă
7	Criptarea și anonimizarea a datelor.	Recomandare fermă
8	Ținerea evidenței prelucrărilor de date.	Recomandare fermă
9	Implementarea unor soluții de backup.	Recomandare fermă
10	Contract scris cu furnizorii de servicii IT prin care definim clauze de protecția datelor la care le dam acces.	Recomandare fermă

1. Desemnarea unui ofițer de protecția datelor - DPO - până la 25 mai 2018

Acesta poate fi un angajat din interiorul Primăriei (chiar Primarul însuși) sau un contractat extern.

Responsabilul cu protecția datelor nu poate fi sancționat nici concediat pentru îndeplinirea atribuțiilor sale. Este necesar ca acesta să aibă acces la toate operațiunile de prelucrare a datelor, până la cel mai înalt nivel al conducerii.

În al doilea rând, acesta trebuie instruit pentru a-și putea exercita corespunzător atribuțiile.

După desemnarea unui DPO, acesta trebuie să se înregistreze la Autoritatea de protecția datelor ca și punct de contact al instituției.

2. Raportare a scurgerile de date către autorități în maxim 72 de ore de la identificare

Ce înseamnă o scurgere de date? Înseamnă că datele personale ale cetățenilor ajung unde nu ar avea voie să fie și/sau pe mâinile unor persoane neavizate.

De exemplu, furtul unei baze de date sau ale unor dosare din arhivă; un angajat care își copiază pe stickul USB personal documente care conțin date cu caracter personal și le pune la dispoziția unor terți.

Cum îmi dau seama că a avut loc o scurgere de date? Ei bine, aici intervine rolul următoarelor recomandări cu privire la proceduri și măsuri tehnice de adoptat. Chiar dacă ele nu sunt specificate ca fiind obligatorii, în lipsa lor riscul unei scurgeri de date pe care să nu se poata identifica (și deci raporta) crește exponențial.

La care autoritate se raporteza mai exact scurgerea de date? În cazul Romaniei, la Autoritatea Natională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

3. Inventarierea în scris a echipamentelor din cadrul Instituției.

Este neceara o Inventariere în scris a datelor cu caracter personal pe care le procesam, fluxurile acestor date și echipamentele din cadrul Instituției.

Este recomadat să realizam un inventar atât al tuturor datelor cu caracter personal pe care instituția le colectează cât și al tuturor fluxurilor de date și al proceselor de prelucrare. În acest sens sunt importante caracteristicile acestor date: ale cui sunt datele, care est scopul și temeiul legal pentru această procesare, unde sunt stocate, măsurile și procedurile de securitate, cine le operează și cine are acces la ele, etc.

Pentru a veni în ajutorul comunelor s-a creeat GDPR Complet Cartografiere Date cu Caracter Personal – o aplicație software creată special pentru cartografierea datelor și realizarea unei hărți cu aceste date și fluxurile / legăturile dintre ele.

Un aspect la fel de important este și inventarierea echipamentelor din cadrul instituției: calculatoarele, serverele și laptopurile pe care se lucrează, dar și telefoane mobile, routere, hard diskuri externe, stickuri USB, etc.

Trebuie realizată o inventarie atât hardware cât și software a acestor echipamente. În acest sens exista o aplicație care permite realizarea acestui audit: GDPR Audit.

4. Definire a temeiului legal de colectare a datelor

În cazul Primariei situația este simplă. Temeiul legal se încadrează în special la una din cele șase variante de temei menționate de regulament și anume:

Executarea unei sarcini care serveşte unui interes public

Mai concret, Instituția nu ar colecta taxe și impozite dacă nu ar avea acces la datele cetatenilor cu caracter personal.

Celelalte cinci temeiuri legale în baza cărora se pot procesa date cu caracter personal:

1. Executarea unui contract;
2. Consimțământul;
3. Executarea unei obligații legale ce îi revine operatorului;
4. Prelucrarea este necesară pentru protejarea unor interese vitale ale persoanei vizate sau ale altei persoane fizice;
5. Prelucrarea este necesară în scopul intereselor legitime urmărite de operator;

5. Evaluarea riscurilor de scurgere de date

Evaluarea aceasta presupune o analiză (de bun simț)în care ne gândim ce fel de date personale se pot scurge cel mai ușor și pe unde anume?

Câteva posibile exemple de zone de risc într-o primărie:

- Dosare care sunt stivuite la vedere și la care poate avea acces oricare din angajați, inclusiv personalul de curațenie.
- Pe rețeaua de calculatoare nu este instalat un antivirus la zi ceea ce o face foarte expusă la atacuri prin care se pot fura datele de pe calculatoarele din rețea

- Orice angajat poate veni cu un memory stick de acasă și copia pe el orice fel de date de pe calculatoarele instituției. Sau să aducă (fie și neintenționat) un virus pe care să-l introducă în rețeaua IT a Primăriei.

Exemplele de acest gen reprezintă niște riscuri brutale de scurgere sau periclitare a datelor cu caracter personal pe care trebuie să le identificam prin această analiză. Asta pentru că în cazul unui control să putem demonstra că am luat măcar un set minim de măsuri pentru a le preveni.

6. Formularea în scris a unui set de proceduri tehnice și de conduită pentru prelucrarea datelor

Acest set de proceduri are ca rol

- Oferirea unei priviri de ansamblu transparente, în scris, a felului în care sunt colectate și procesate datele și de către cine anume
- Să dea un set de soluții clare la riscurile identificate la evaluarea de la punctul 5.

De exemplu o măsură de bun simț în cazul stivelor de dosare la care are nepermis de multă lume acces ar fi ca ele să fie ținute într-un dulap încuiat iar cheia să fie doar la doua sau trei persoane pe care le desemnam.

E vreun anumit format pe care trebuie să îl respect aici?

Regulamentul nu impune neapărat o structură vizuală, mai degrabă una de substanță a conținutului. Și anume în documentul respectiv trebuie să apară:

- Ce fel de date sunt colectate? (ex: nume, prenume, adresă, serie și nr CI, CNP)
- De ce anume? Pentru ce se folosesc (temeiul legal)
- Cine le prelucrează?
- Cum sunt ele securizate?

7. Criptare și anonimizare a datelor

Aici intrăm într-o zonă mai tehnică unde e bine să fie implicatii specialisti IT. Și anume vorbim de bazele de date în care se regăsesc datele personale ale cetățenilor.

Acestea pe de-o parte trebuie construite astfel încât să asigure anonimizarea datelor. Mai concret, să nu existe într-un sigur loc (aceeași tabelă) TOATE datele unei persoane, ci în mai multe tabele. Acestea din urmă ar urma să fie unificate de către aplicația care le folosește pe baza unor id-uri.

În al doilea rând, bazele de date trebuie criptate astfel încât informația din interiorul lor să nu fie accesibilă fără accesul la un cod de criptare (encryption key). În acest sens se pot folosi aplicații de criptare.

În acest sens este recomandat să contactam furnizorii de aplicații și să verificam daca implementează măsuri în direcția aspectelor de mai sus.

8. Ținere evidența prelucrărilor de date

Pentru a putea identifica o scurgere de date, e foarte important să poți afla că aceasta s-a produs dar și pe unde anume a avut loc. Aici intervine utilitatea unei soluții de evidență a prelucrării datelor.

Această evidență devine cu atât mai importantă cu cât volumul datelor prelucrate este mai mare deși este mai greu de ținut în lipsa unei soluții performante în acest sens.

In întâmpinarea necesității de evidențiere și monitorizare a activităților de prelucrare a datelor cu caracter personal exista două aplicații specializate în acest sens: GDPR Complet Audit și GDPR Complet Cartografiere Date cu Caracter Personal.

9. Implementare soluții de backup a datelor

Acestea ne vor ajuta să avem o versiune a datelor la zi, în cazul pierderii sau coruperii datelor pe care le deținem

Sunt multiple soluții în acest sens, de la aplicații gratuite gen Dropbox sau Google Drive până la variante personalizate care pot fi oferite de furnizorii de servicii IT.

Trebuie acordata atenție la contractele cu furnizorii de servicii IT.

10. Existenta unui contract scris cu furnizorii de servicii IT prin care sa definim clauzele de protecția datelor la care le dam acces

GDPR ne obligă să avem un contract scris cu aceștia (atât furnizorii de servicii IT, cât și cu furnizorii aplicațiilor pe care le folosim – cei care au în definitiv acces la datele Instituției) prin care se stabilește clar responsabilitatea lor în protejarea datelor la care le dam acces.

Conform regulamentului, deși aceștia nu sunt operatori de date, ei sunt denumiți ca **împuterniciți** și, având acces la datele institutiei poartă și ei o răspundere importantă, care trebuie clarificată prin contractul scris (fie printat, fie doar în format electronic) pe care îl semnam cu aceștia.

Este foarte recomandat ca și ei ca firmă furnizoare de produse sau servicii să fie în conformitate cu GDPR.

Intocmit –secretar UAT

Fagarasan Simona