PACHIU & ASSOCIATES

ATTORNEYS AT LAW · RECHTSANWÄLTE · ABOGADOS

B.E.L.I.E.V.E.

***B**ound by **E**xcellence, as **L**inks in a **C**hain, we create **I**nnovation from **E**nthusiasm and **V**alue from **E**xpertise.*

SECURITATEA DATELOR CU CARACTER PERSONAL

B.E.L.I.E.V.E.

***B**ound by **E**xcellence, as **L**inks in a **C**hain, we create **I**nnovation from **E**nthusiasm and **V**alue from **E**xpertise.*

SANCTIUNI APLICATE DE ANSPDCP

- **20.000 lei-** BNP- s-a constatat ca operatorul nu a adoptat suficiente masuri de securitate si confidentialitate pentru a asigura protectia datelor personale ale clientilor, angajatilor si colaboratorilor sai (inclusiv categorii de date cu caracter special) impotriva dezvaluirii si a accesului neautorizat, precum si impotriva oricarei alte forme de prelucrare ilegala, ceea ce a condus la dezvaluirea pe Internet a datelor cu caracter personal ale acestora, cu incalcarea dispozitiilor art. 19 si art. 20 din Legea nr. 677/2001
- **7.500 lei-** DVBL 2- pentru neindeplinirea obligatiilor privind confidentialitatea si aplicarea masurilor de securitate din Legea nr. 677/2001
- **10.000 lei-** OPERATOR DE TELEFONIE MOBILA- s-a constatat faptul ca, in memoria telefonului primit de la service, se aflau date cu caracter personal de la utilizatorii precedenti: logare automata pe Facebook, numere de telefon si mesaje personale, inclusiv balanta conturilor bancare. Urmare a acestei situatii, petentul a sesizat telefonic operatorul, insa a precizat ca sesizarea sa nu a fost luata in seama. In cadrul investigatiei s-a constatat ca S.C. OR S.A. nu a luat masurile necesare pentru a preveni dezvaluirea sau accesul neautorizat la datele cu caracter personal stocate pe telefonul primit de la service, proprietatea SC OR SA

SANCTIUNI LEGALE

- **LEGEA NR. 677/2001**

  15.000-50.000 RON

  Neindeplinirea obligatiilor privind aplicarea masurilor de securitate si de pastrare a confidentialitatii-

- **PROIECTUL DE REGULAMENT EUROPEAN**

  pana la **1.000.000 euro sau 2% din cifra de afaceri**

  Neadoptarea de norme interne sau nepunerea in aplicare de masuri corespunzatoare pentru a asigura si demonstra conformitatea cu art. 30

CE INSEAMNA PRELUCRARE DE DATE?

- Orice operatiune care se efectueaza asupra datelor cu caracter personal prin mijloace automate sau neautomate, precum colectarea, inregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, transmiterea catre terti, diseminare sau in orice alt mod, alaturarea, combinarea, blocarea, stergerea sau distrugerea.

SIGURANTA DATELOR

- Orice operator de date este obligat sa aplice **masurile tehnice si organizatorice adecvate** pentru protejarea datelor cu caracter personal impotriva:
- distrugerii accidentale sau ilegale;
- pierderii;
- modificarii;
- dezvaluirii; sau
- accesului neautorizat in special daca prelucrarea comporta transmisii de date in cadrul unei retele, precum si impotriva oricarei alte forme de prelucrare ilegala.

CERINTE MINIME DE SECURITATE

- vor fi elaborate de autoritatea de supraveghere si vor fi actualizate periodic, corespunzator progresului tehnic si experientei acumulate

- Ordinul 52/2002 al Avocatului Poporului privind aprobarea Cerintelor minime de securitate a prelucrarilor de date cu caracter personal

- Nu exista actualizari, recomandari sau instructiuni noi !!!!

CERINTE MINIME DE SECURITATE

- Identificarea si autentificarea utilizatorului
- Tipul de acces
- Colectarea datelor
- Executia copiilor de siguranta
- Computerele si terminalele de acces
- Fisierele de acces
- Sistemele de telecomunicatii
- Imprimarea datelor
- Instruirea personalului
- Folosirea computerelor

CERINTE MINIME DE SECURITATE IN SECTORUL COMUNICATIILOR ELECTRONICE

- Furniorul unui serviciu de comunicatii electronice are obligatia de a lua masuri tehnice si organizatorice adecvate , proprotional cu riscul existent, avand in vedere posibilitatile tehnice de ultima ora si costurile implementarii acestor masuri.

- Furnizorul trebuie sa ia masuri pentru:

- A preveni si a minimiza impactul incidentelor de securitate asupra utilizatorilor si asupra retelelor interconectate;
- A garanta integritatea retelelor asigurant astfel continuitatea prestarii serviciilor;
- Sa notifice autoritatea competenta despre orice incalcare a securitatii sau pierdere a integritatii care a avut un impact semnificativ asupra functionalitatii reletelor si serviciilor dar si persoanele afectate de incalcare;
- Sa tina o evidenta a incalcarilor de securitate

POLITICA DE MANAGEMENT AL RISCULUI

- identificarea si evaluarea asset-urilor;
- identificarea si evaluarea vulnerabilitatilor si amenintarilor;
- identificarea si evaluarea riscului final si a nivelului de acceptare a riscului
- tratarea riscului nedorit prin:
  - Diminuare (aplicarea de masuri de control);
  - Transfer (sa ii faci pe altii sa preia raspunderea financiara: asigurare);
  - Acceptare (toleranta) atunci cand costul incalcarii este mult mai mic decat costul diminuarii riscului

B . E . L . I . E . V . E .

PACHIU & ASSOCIATES
ATTORNEYS AT LAW · RECHTSANWÄLTE · ABOGADOS