PACHIU & ASSOCIATES

WWW.PACHIU.COM

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

Bound by Excellence, as Links in a Chain, we create Innovation from Enthusiasm and Value from Expertise.

PACHIU & ASSOCIATES

ATTORNEYS AT LAW · RECHTSANWÄLTE · ABOGADOS

AUDITUL IN MATERIA DATELOR CU CARACTER PERSONAL

Mihaela Cracea, Managing Associate

14 IUNIE 2016

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

Bound by Excellence, as Links in a Chain, we create Innovation from Enthusiasm and Value from Expertise.

NEW LEGAL FRAMEWORK
2018

DIRECTIVA 95/46/EC

REGULAMENTUL EUROPEAN PRIVIND PROTECTIA DATELOR NR. 679/2016

Accountability

- a putea sa demonstrezi ca actionezi in conformitate cu cerintele legale
- acceptarea responsabilitatii pentru felul in care sunt procesate datele cu caracter personal
- organizatia ”accountable” este acea organizatie care are implementate politici si proceduri adecvate care promoveaza bunele practici in materie de protectie a datelor si care, luate impreuna, constituie un program de privacy management

PROCEDURA DE AUDIT

I verifica daca prelucrezi date cu caracter personal

II verifica pentru cine prelucrezi date: operator si/sau imputernicit

III decide daca vrei sa afli daca esti *compliant* (costuri: timp si bani)

IV prezinta problema factorilor de decizie, prezinta riscurile si obtine decizia de management

IV propune-ti un deadline pt finalizarea auditului

V stabileste echipa: interna sau externa

VI verifica periodic stadiul procesului de audit

VII studiaza raportul de audit: concluzii si recomandari

PROCEDURA DE AUDIT

VIII analizeaza riscul vs. costurile pe care a fi *compliant* le implica:

10 mil euro sau 2% din CA globala

20 mil euro sau 4% din CA globala

operatorii de date vor implementa masuri tehnice si organizatorice adecvate in vederea asigurarii unui nivel de securitate corespunzator, tinand seama de stadiul actual al dezvoltarii, de costurile implementarii, contextul si scopurile prelucrarii, de risc pentru drepturile si libertatile persoanelor fizice

VIII decide daca vrei sa devii *compliant*

IX activeaza procese si proceduri, politici, drafturi de documente, implementeaza sesiuni de training de personal; traseaza sarcini si responsabilitati ca sa fii pregatit pentru intrarea in vigoare a regulamentului;

X controleaza periodic respectarea lor (factorul uman)

CONTINUTUL AUDITULUI

I identificarea diverselor tipuri de date prelucrate

II identificarea persoanelor vizate

III identificarea scopurilor prelucrarii

IV identificarea persoanelor care au acces la date

V verificarea daca prelucrarea se face tinand seama de principiile legale: legalitate, corectitudine, transparenta, limitarea scopului, minimizarea datelor, acuratete, limitarea stocarii, integritate si confidentialitate (“accountability”)

VI verificarea obtinerii consimtamantul persoanei vizate sau, dupa caz, informarii persoanele vizate cu privire la prelucrare

VII verificarea modului in care persoanele vizate au fost informate sau li s-a obtinut consimntamantul (probleme speciale apar in cazul prelucrarii de date in scop de marketing direct, in scop de profiling)

CONTINUTUL AUDITULUI

VIII verificarea respectarii drepturilor persoanelor vizate, respectiv: dreptul de acces, dreptul de a cere rectificarea datelor, dreptul de stergere (the right to be forgotten), dreptul de a se opune prelucrarii, dreptul la portabilitatea datelor, dreptul de a obiecta asupra prelucrarii

IX verificarea existentei (daca este necesar) unei evidente a prelucrarilor (din 2018): potrivit noului regulament, existenta unui raport, a unei evidente a tuturor prelucrarilor (daca veti peste 250 salariati, daca prelucrarea prezinta riscuri mari la adresa drepturilor si libertatilor persoanelor; prelucrarea nu este ocazionala, sau presupune prelucrare de date cu caracter special

CONTINUTUL AUDITULUI

X verificarea aplicarii masurilor de securitate cerute de lege pentru a se asigura:

- pseudonimizarea și criptarea datelor cu caracter personal
- confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare
- capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea in timp util in cazul in care are loc un incident de natura fizica sau tehnica
- testarea, evaluarea și aprecierea periodice ale eficacitatii masurilor tehnice și organizatorice pentru a garanta securitatea prelucrării

X verifica daca trebuie sa respecti regula “data privacy *by design* si *by default*”

CONTINUTUL AUDITULUI

verificarea existentei de template-uri, proceduri, politici;

XII verificarea existentei unei proceduri de evaluare a riscului in cazul anumitor tipuri de prelucrari (ex: in cazul evaluarii persoanelor ca urmare a prelucrarilor automate de date)

XIII verificarea transferurilor de date si mecanismele de transfer si corelarea dintre transfer scriptic si real

XIV daca se impune numirea unui responsabil cu protectia datelor

Daca ati realizat toate acestea, veti putea demonstra usor autoritatii de control ca sunteti

“**accountable**”

CONTACT

75 – 77 Buzesti St, 5th floor
Bucharest, 011013
Tel: +40 21 312 10 08

mihaela.cracea@pachiu.com
pr@pachiu.com

www.pachiu.com