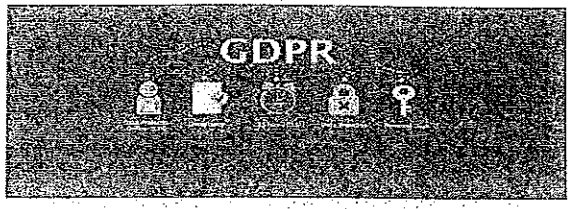

GDPR | General Data Protection Regulation

Nr. 8953 din 28.12.2023

În atenția
Conducerii instituției, Responsabilului cu Protecția Datelor și angajaților

MATERIAL DE INSTRUIRE A PERSONALULUI
Privind protecția datelor cu caracter personal

Având în vedere posibilele incidente de securitate a prelucrării datelor cu caracter personal și necesitatea inițierii măsurilor de reacție conform obligațiilor legale prevăzute de Regulamentul UE 679/2016 – GDPR, vă comunicăm o situație cu risc real de materializare în cazul operatorilor din domeniul public, în scopul conștientizării personalului Dumneavoastră și a Responsabilului cu Protecția Datelor Personale – DPO..

*
* *

Pe pagina de facebook a unei persoane fizice, a fost publicat un document intern al unei instituții publice - nedestinat publicării - care conținea date cu caracter personal ale conducerii operatorului și ale unor angajați.

Documentul, un convocator destinat înștiințării unor angajați cu privire la planificarea unei ședințe interne, cuprindea următoarele tipuri de date cu caracter personal numele, prenumele, funcția, locul de muncă , apartenența sindicală (date cu caracter special) și semnăturile conducerii operatorului.

La scurt timp după postarea pe pagina de facebook, un angajat a sesizat conducerea operatorului și Responsabilul cu Protecția Datelor – DPO privind publicarea documentului respectiv.

Practic, prin divulgarea acestui document, angajatul operatorului care a transmis documentul către proprietarul paginii de Facebook a încălcat clauzele contractuale, regulamentul intern și procedura privind confidențialitatea, devenind operator de date cu caracter personal fără a respecta obligațiile de legalitate specificate de GDPR la art.6 și modificând scopul în care operatorul prelucrează date cu caracter personal.

În conformitate cu art. 3, 12 din GDPR divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate de operator, sau accesul neautorizat la acestea constituie o încălcare a securității datelor ce poate fi investigată și sancționată inclusiv cu amenzi de către ANSPDCP, în baza competențelor stabilite de GDPR și a Legii 190/2018.

Conform atribuțiilor prevăzute de GDPR, Responsabilul cu Protecția Datelor a pus în aplicare Planul de Reacție la Incidentele de Securitate, astfel:

- Verificarea contului de facebook care a publicat documentul, realizarea unei capturi de ecran cu documentul publicat și comentariile online, pentru stabilirea identității persoanei care-l utilizează;

- Consemnarea şi documentarea incidentului de securitate în Registrul DPO anexat Planului de Reacţie la Incidentele de Securitate;
- Identificarea tuturor persoanelor vizate - destinatarii convocatorului, a căror date cu caracter personal au fost divulgate;
- Transmiterea către toţi destinatarii convocatorului, precum şi către proprietarul contului de Facebook a unei Notificări de Confidenţialitate cu privire la ilegalitatea publicării acestui document şi evitarea prejudicierii persoanelor vizate (model anexat Planului de Reacţie la incidente de Securitate). Notificarea proprietarului contului de Facebook a fost realizată prin postarea Notificării de Confidenţialitate pe site-ul oficial al operatorului cu solicitarea ştergerii documentului divulgat ilegal;
- Notificarea ANSPDCP, conform art.33 GDPR, în maxim 72 de ore de la sesizarea incidentului. DPO propune sesizarea ANSPDCP de către conducătorul operatorului prin completarea formularului online de pe site-ul www.dataprotection.ro semnat electronic – Notificare breşă: https://www.dataprotection.ro/formulare/formularBresaGdpr.do .

În scopul conştientizării angajaţilor cu privire la aspectele de confidenţialitate, după identificarea angajatului care a divulgat documentul, acesta a fost sancţionat disciplinar conform prevederilor Codului Muncii şi a Codului Administrativ, sancţiunea aplicată şi motivele aplicării fiind comunicată angajaţilor fără a se preciza datele de identificare a persoanei sancţionată disciplinar.

De asemenea, în urma sesizării ANSPDCP de către operator, autoritatea a demarat investigaţii pentru aplicarea prevederilor legale proprietarului contului de Facebook.

*

* *

CONCLUZII
privind
Gestionarea incidentelor de securitate

Nu se fac copii ale documentelor interne şi nu se diseminează în exterior decât de personalul cu atribuţii, conform obligaţiilor legale ale operatorului şi după consultarea DPO.

Incidentul de securitate a datelor cu caracter personal este o încălcare care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea.

Orice incident de securitate sau suspiciune se raportează verbal sau scris direct DPO de către personal.

Consecinţele unui incident de securitate, dacă nu există o reacţie imediată (maxim 72 de ore de la constatare), pot crea riscuri mari pentru operator - de la costuri de reputaţie până la amenzi aplicate de ANSPDCP în baza GDPR şi Legii 190/2018.

În situaţia în care are loc un incident de securitate, se impune aplicarea de către Operator a unor măsuri conform Planului de Reacţie la Incidentele de securitate – gestionat de echipa coordonată de DPO.

*

* *

Aspecte legale incidente în speță:

GDPR
Articolul 3
12. „încălcarea securității datelor cu caracter personal" înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

Articolul 33
Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal
(1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente în temeiul articolului 55, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată din partea autorității de supraveghere în cazul în care.
(2) Persoana împuternicită de operator înștiințează operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.
(3) Notificarea menționată la alineatul (1) cel puțin:
(a) descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
(b) comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
(c) descrie consecințele probabile ale încălcării securității datelor cu caracter personal;
(d) descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.
(4) Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.
(5) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu prezentul articol.

Articolul 34
Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal
(1) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

(2) În informarea transmisă persoanei vizate prevăzută la alineatul (1) din prezentul articol se include o descriere într-un limbaj clar şi simplu a caracterului încălcării securităţii datelor cu caracter personal, precum şi cel puţin informaţiile şi măsurile menţionate la articolul 33 alineatul (3) literele (b), (c) şi (d).
(3) Informarea persoanei vizate menţionată la alineatul (1) nu este necesară în cazul în care oricare dintre următoarele condiţii este îndeplinită:
(a) operatorul a implementat măsuri de protecţie tehnice şi organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securităţii datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;
(b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile şi libertăţile persoanelor vizate menţionat la alineatul (1) nu mai este susceptibil să se materializeze;
(c) ar necesita un efort disproporţionat. În această situaţie, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.
(4) În cazul în care operatorul nu a comunicat deja încălcarea securităţii datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securităţii datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condiţiile menţionate la alineatul (3) sunt îndeplinite.

ORDONANTA DE URGENTA NR. 57 privind Codul administrativ

Articolul 8
Principiul transparentei
(1) In procesul de elaborare a actelor normative, autoritățile si instituțiile publice au obligația de a informa si de a supune consultării si dezbaterii publice proiectele de acte normative si de a permite accesul cetățenilor la procesul de luare a deciziilor administrative, precum si la datele si informațiile de interes public, in limitele legii.
(2) Beneficiarii activităților administrației publice au dreptul de a obține informații de la autoritățile si instituțiile administrației publice, iar acestea au obligația corelativa a acestora de a pune la dispoziția beneficiarilor informații din oficiu sau la cerere, in limitele legii.

Articolul 434
Loialitatea fata de autoritățile si instituțiile publice
(1) Funcționarii publici au obligația de a apăra in mod loial prestigiul autoritarii sau instituției publice in care își desfășoară activitatea, precum si de a se abține de la orice act ori fapt care poate produce prejudicii imaginii sau intereselor legale ale acesteia.
(2) Funcționarilor publici le este interzis:
a) sa exprime in public aprecieri neconforme cu realitatea in legătura cu activitatea autoritarii sau instituției publice in care își desfășoară activitatea, cu politicile si strategiile acesteia ori cu proiectele de acte cu caracter normativ sau individual;

Articolul 439
Păstrarea secretului de stat, secretului de serviciu si confidențialitatea
Funcționarii publici au obligația sa păstreze secretul de stat, secretul de serviciu, precum si confidențialitatea in legătura cu faptele, informațiile sau documentele de care iau cunoștința

in exercitarea funcţiei publice, in condiţiile legii, cu aplicarea dispoziţiilor in vigoare privind liberul acces la informaţiile de interes public.

Articolul 492
Răspunderea administrativ-disciplinara
(1) Încălcarea cu vinovăţiei de către funcţionarii publici a îndatoririlor corespunzătoare funcţiei publice pe care o deţin si a normelor de conduita profesionala si civica prevăzute de lege constituie abatere disciplinara si atrage răspunderea administrativ-disciplinara a acestora.
(2) Constituie abateri disciplinare următoarele fapte:
.....
e) intervenţiile sau stăruinţele pentru soluţionarea unor cereri in afara cadrului legal;
f) nerespectarea secretului profesional sau a confidenţialităţii lucrărilor cu acest caracter;
g) manifestări care aduc atingere prestigiului autoritarii sau instituţiei publice in care funcţionarul public îşi desfăşoară activitatea;

CODUL MUNCII

Articolul 39
(2) Salariatului îi revin, în principal, următoarele obligaţii:
c) obligaţia de a respecta prevederile cuprinse în regulamentul intern, în contractul colectiv de muncă aplicabil, precum şi în contractul individual de muncă;
d) obligaţia de fidelitate faţă de angajator în executarea atribuţiilor de serviciu;
f) obligaţia de a respecta secretul de serviciu;
Articolul 40
(2) Angajatorului îi revin, în principal, următoarele obligaţii:
e) să constate săvârşirea abaterilor disciplinare şi să aplice sancţiunile corespunzătoare, potrivit legii, contractului colectiv de muncă aplicabil şi regulamentului intern;
i) să asigure confidenţialitatea datelor cu caracter personal ale salariaţilor.

Răspunderea disciplinară
Articolul 247
(1) Angajatorul dispune de prerogativă disciplinară, având dreptul de a aplica, potrivit legii, sancţiuni
disciplinare salariaţilor săi ori de câte ori constată că aceştia au săvârşit o abatere disciplinară.
(2) Abaterea disciplinară este o faptă în legătură cu munca şi care constă într-o acţiune sau inacţiune săvârşită cu vinovăţie de către salariat, prin care acesta a încălcat normele legale, regulamentul intern, contractul individual de muncă sau contractul colectiv de muncă aplicabil, ordinele şi dispoziţiile legale ale conducătorilor ierarhici.

Articolul 248
(1) Sancţiunile disciplinare pe care le poate aplica angajatorul în cazul în care salariatul săvârşeşte o abatere disciplinară sunt:
a) avertismentul scris;
b) retrogradarea din funcţie, cu acordarea salariului corespunzător funcţiei în care s-a dispus retrogradarea, pentru o durată ce nu poate depăşi 60 de zile;
c) reducerea salariului de bază pe o durată de 1-3 luni cu 5-10%;
d) reducerea salariului de bază şi/sau, după caz, şi a indemnizaţiei de conducere pe o perioadă de 1-3 luni cu 5-10%;

e) desfacerea disciplinară a contractului individual de muncă.
(2) În cazul în care, prin statute profesionale aprobate prin lege specială, se stabileşte un alt regim sancţionator, va fi aplicat acesta.
(3) Sancţiunea disciplinară se radiază de drept în termen de 12 luni de la aplicare, dacă salariatului nu i se aplică o nouă sancţiune disciplinară în acest termen. Radierea sancţiunilor disciplinare se constată prin decizie a angajatorului emisă în formă scrisă.

Legea nr. 544 / 2001

ART. 12
(1) Se exceptează de la accesul liber al cetăţenilor, prevăzut la art. 1 şi, respectiv, la art. 11^1, următoarele informaţii:
---
a) informaţiile din domeniul apărării naţionale, siguranţei şi ordinii publice, dacă fac parte din categoriile informaţiilor clasificate, potrivit legii;
b) informaţiile privind deliberările autorităţilor, precum şi cele care privesc interesele economice
şi politice ale României, dacă fac parte din categoria informaţiilor clasificate, potrivit legii;
d) informaţiile cu privire la datele personale, potrivit legii;
(2) Răspunderea pentru aplicarea masurilor de protejare a informaţiilor aparţinând categoriilor prevăzute la alin. (1) revine persoanelor şi autorităţilor publice care deţin astfel de informaţii, precum şi instituţiilor publice abilitate prin lege să asigure securitatea informaţiilor.

Întocmit,
Responsabil cu Protecţia Datelor

Notă:
Documentul se păstrează în format electronic la DPO.
După listare, luare la cunoştinţă şi înregistrare se păstrează la DPO sau HR pentru a dovedi instruirea periodică a personalului în domeniul protecţiei datelor.