HIDROELECTRICA

Hidroelectrica S.A.
Societate administrată în sistem dualist
J40/7426/2000
RO 13267213
Capital social: 4.481.650.630 lei
Certificat ISO 9001/14001/OHSAS 18001
SRAC Nr. 325; Nr. 95; Nr. 250

NOTĂ

către Adunarea Generala a Acționarilor SPEEH Hidroelectrica SA

1. Titlu: Informarea acționarilor SPEEH Hidroelectrica SA privind stadiul masurilor luate pentru asigurarea conformității cu Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)

2. Tip notă:

INFORMARE	**x**	**Adunarea Generală a Acţionarilor**

3. Hotărâre propusă.

Informarea Adunării Generale a Acționarilor Hidroelectrica privind măsurile tehnice și organizatorice care sunt și vor fi întreprinse la nivelul SPEEH Hidroelectrica SA cu privire a conformitatea cu Regulamentul UE 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

4. Temei legal.

- Art. 117^2 alin. (3) din Legea nr. 31/1990 – Legea Societăților Comerciale
- Regulamentul UE 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

5. Conţinut.

Având în vedere solicitarea acționarului majoritar din adresa înregistrată la Hidroelectrica S.A. sub nr. 25498/09.03.2018, vă aducem a cunoștință următoarele:

În temeiul Regulamentului 679/2016 au fost organizate mai multe sesiuni de lucru la nivelul Hidroelectrica începând din trimestrul 4, 2017.

La începutul lunii februarie, 2018, în temeiul Referatului 11758, **din 5 februarie 2018**, privind Măsurile organizatorice pentru derularea proiectului "Asigurarea compatibilității cu Regulamentul General privind protecția datelor cu caracter personal (RGDP) - Regulamentul UE 2016/679" au fost stabilite **Echipa de proiect (formată din Comitetul director și Echipa de implementare) și Echipa de implementare** care participă la asigurarea acestei conformități. Comitetul director cuprinde managerii de departament, directorii de sucursale, șefi de serviciu și alte persoane considerate relevante pentru scopul proiectului. Echipa de implementare cuprinde personalul din

departamentele Hidroelectrica și din sucursale care au fost desemnați să asigure derularea acestui demers de conformitate.
Referatul definește scopul proiectului și modul de lucru.
În baza deciziei 191/8 februarie 2018, au fost nominalizate: Echipa de proiect, dar și Directorul de proiect care va asigura și funcția de Ofițer responsabil de protecția Datelor (DPO). Aceste două responsabilități vor fi asigurate de Managerul departamentului de Risc Management din cadrul Hidroelectrica. Cumulul de funcții DPO cu manager de risc întrunește cerințele de conformitate prevăzute de Regulamentul 679/2016 dar și recomandările Ghidului privind Responsabilul cu protecția datelor ('DPOs') 16/RO WP 243 rev.01 , elaborat de Grupul de lucru „articolul 29" pentru protecția datelor, și revizuit și adoptat în data de 5 aprilie 2017

Măsurile luate până la acest moment au vizat:
- distribuirea și colectarea unui **chestionar detaliat la nivelul tuturor departamentelor** și sucursalelor din cadrul Hidroelectrica pe tema datelor cu caracter personal;
- **popularizarea subiectului** la nivelul tuturor departamentelor și sucursalelor prin sesiuni de informare și discuții individuale;
- **identificarea fluxurilor de date cu caracter personal;**
- identificarea **tipurilor de date procesate, a procesatorilor, a temeiurilor** care stau la baza procesării, **a perioadei de stocare;**
- identificarea **datelor personale cu caracter special** care sunt procesate (ex copii, caziere, certificate medicale, etc);
- **identificarea vulnerabilităților** aferente procesărilor precum și a resurselor **și măsurilor necesare** (din punct de vedere al proceselor, al securității fizice și al securității cibernetice/IT);
- realizarea **primelor drafturi de registre de evidență a activităților de prelucrare** conform cerințelor de art. 30 din Regulamentul 679/2016;
- **măsuri imediate și/sau actualizarea procedurilor** din zonele senzitive (IT, resurse Umane, Securitate, Administrarea patrimoniului etc.) cu prevederi speciale în spiritul Regulamentului 679/2016;
- **introducerea prevederilor și cerințelor de GDPR la nivelul procedurilor de sistem HP-SCIM;**
- transmiterea de **notificări către Hidroserv SA** cu privire la stadiul implementării măsurilor de conformitate cu Regulamentul 679/2016.

Măsuri în derulare la data realizări acestei informări
- **realizarea de către DPO unui set de recomandări** și asumarea de către managerii de departament și a directorilor de sucursale a măsurilor necesare pentru asigurarea conformității pe marginea tuturor spețelor identificate;
- **realizarea unui suport de curs** în format electronic și fizic și **examinarea tuturor angajaților** Hidroelectrica pe acest subiect cu scopul asigurării informării cu privire la drepturile și obligațiile angajaților Hidroelectrica, la toate nivelurile;
- **actualizarea fișelor de post individuale și a ROF- ului Hidroelectrica** cu cerințele minimale specifice aferente prevederilor Regulamentului 679/2016;
- **stabilirea planurilor de acțiune cu calendar de implementare** și responsabilitățile aferente pe toată durata anului în curs, la nivel de departament plecând de la situațiile și vulnerabilitățile

identificate. (ex: securitatea fizică asigurată dosarelor de personal, pseudonimizarea datelor cu caracter personal înregistrate în SAP, asigurarea protecției datelor începând cu momentul conceperii și în mod implicit - să nu mai solicităm date cu caracter personal care nu sunt absolut necesare, etc);

- **identificarea și stabilirea resurselor necesare la nivel de proces/departament** pe următoarea structură:
  - **modificări de fluxuri de proces** (ex notificarea autorității de supraveghere în cazul scurgerilor de date care se produc la terți cărora le-am transmis date cu caracter personal);
  - **suport juridic** (de tipul formularului de consimțământ, cauză contractuală etc);
  - **suport IT** (instrumente de IT care să ajute identificarea manipulării, la accesul segregat și monitorizat al datele cu caracter personal din tot sistemul IT al Hidroelectrica, identificarea resurselor de asigurare a conformității pentru sistemele IT moștenite, etc);
- realizarea caietelor de sarcini și a **achizițiilor pentru atragerea resurselor**, acolo unde este necesar și nu pot fi asigurate prin resurse interne;
- **instituirea modalităților de verificare a respectării cerințelor prevăzute de Regulamentul 679** (ex: audituri și verificări inopinate cu privire la respectarea politicii de birouri curate/goale, teste de penetrare, audituri IT etc.);
- realizarea unor **chestionare de evaluare a terților** către care transmitem date cu caracter personal, mai ales dacă acești terți nu sunt autorități ale statului sau entități certificate ca fiind conforme cu GDPR (regulamentul 679/2016);
- **analiza și stabilirea oportunității de derulare a evaluării impactului asupra protecției datelor și consultarea prealabilă** conform prevederilor de la articolul 35 din Regulamentul 679/2016;
- **analiza și stabilirea oportunității de certificare pentru alte standarde ISO (ex: 27001-5)** care certifică din punct de vedere IT întrunirea unor condiții de conformitate inclusiv cu cerințele Regulamentului 679/2016;
- **realizarea evaluărilor de risc** stabilite de Regulamentul 679;
- **înregistrarea la Autoritatea** Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal;
- **realizarea unei proceduri de lucru master** care să prevadă modul de actualizare a registrului de evidență, modul de escaladarea a situațiilor, modul de răspuns la solicitările venite din partea persoanelor fizice, etc.

6. Follow-up.

Pașii următori avuți în vedere pe măsura actualizării, prevederilor legale cu privire la aceste subiecte:

- **achiziționarea unor sisteme informatice** care vor fi necesare pentru conformitatea cu recomandările de securitate informatică care derivă din cadrul Regulamentului 679. (ex: sistemele de tip DLP Data Loss Prevention, sisteme de protecție și criptare a datelor alături de sisteme de monitorizare de tip SIEM.

- **documentarea și achiziționarea la nivelul Hidroelectrica unui DMS** (Document management system) - Sistem de gestionare a documentelor care să permită în plus, față de caracteristicile și beneficiile specifice unui astfel de sistem, marcarea documentelor care conțin date cu caracter

personal pentru o evidență conformă și o procesare a acestora, în siguranță, din toate punctele de vedere.

- **certificarea Hidroelectrica ca entitate în conformitate cu cerințele GDPR** în spiritul Regulamentului 679/2016 (încă nu există corpuri de certificare la nivelul UE și nici la nivelul României)

- **certificarea DPO ului Hidroelectrica în conformitate cu cerințele GDPR** în spiritul Regulamentului 679/2016 (singurele certificări sunt cele în baza directivei vechi și a legii din 2001)

- **aderarea la coduri de conduită ale furnizorilor de energie electrică** pe măsură ce vor fi disponibile la nivelul pieței din România.

7. Adunarea Generală a Acţionarilor

Informare

8. Anexe.
Nu este cazul.

Cu stimă,

Bogdan-Nicolae BADEA
Preşedinte Directorat

Marian BRATU
Membru Directorat

Bogdan ŞOŞOACĂ
Membru Directorat

Adrian Constantin VOLINTIR
Membru Directorat

Răzvan Ionuţ Paţaliu
Membru Directorat

Întocmit
Răzvan Tudor
DPO și Manager departament Risc Management

Vizat
Daniela Dunel-Stancu
Manager Departament