Se aproba,

Cosmin Ghita,

Director General,

Avizat,

Mihai Sandulescu,

Director DAMR

NOTA DE INFORMARE
catre actionari privind implementarea Regulamentului 2016/679 (GDPR – Regulamentul general privind protectia datelor) in cadrul SN Nuclearelectrica SA

1. Context

Regulamentul 2016/679[1] a fost emis in scopul realizarii unei mai bune protectii a drepturilor si libertatilor fundamentale a persoanelor fizice (in speta a protectiei persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal), dar si cu scopul uniformizarii acestei protectii si a cadrului legislativ la nivelul Uniunii Europene, si in ceea ce priveste cetatenii UE din aceasta perspectiva, chiar daca operatorii datelor se situeaza in afara Uniunii.

Data fiind complexitatea conformarii cu Regulamentul si costurile semnificative pentru operatorii care prelucreaza date cu caracter personal (e.g. asigurari, banci, servicii de date, servicii medicale), a fost instituit un termen de doi ani (de la emiterea Regulamentului, in 27.04.2016, si pana la data de 25.05.2018) in care organizatiile carora li se aplica Regulamentul trebuie sa ia toate masurile tehnice si organizatorice pentru conformare.

Regulamentul a intrat in vigoare in mod automat (fara transpunere in legislatia/ dreptul intern/a).

2. Impactul Regulamentului 2016/679 (sumar executiv)

Regulamentul 2016/679 inlocuieste cadrul legislativ anterior (Legea 677/21.11.2001[2] pentru

[1] Regulamentul (UE) 2016/679 al Parlamentului European si al Consiliului din 27.04.2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE (Regulamentul general privind protectia datelor).

[2] Abrogata prin Legea nr. 129/15.06.2018 pentru modificarea si completarea Legii nr 102/2005 privind infiintarea, organizarea si functionarea Autoritatii Nationale de Supraveghere a Prelucrarii Datelor cu Caracter Personal, precum

protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date, si Directiva 95/46/CE), aducand o serie de modificari referitoare la:

a) **aplicabilitate materiala**: Regulamentul se aplica tuturor prelucrarilor de date cu caracter personal (extinderea definitiei datelor cu caracter personal si includerea de noi definitii):
   - prelucrare: orice operatiune sau set de operatiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fara utilizarea de mijloace automatizate, cum ar fi colectarea, inregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispozitie in orice alt mod, alinierea sau combinarea, restrictionarea, stergerea sau distrugerea
   - date cu caracter personal: orice informatii privind o persoana fizica identificata sau identificabila („persoana vizata"); o persoana fizica identificabila este o persoana care poate fi identificata, direct sau indirect, in special prin referire la un element de identificare, cum ar fi un nume, un numar de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale; exemple: nume/ precume, CNP, serie/ numar C.I./ B.I./ pasaport, date medicale, fotografie, adresa de domiciliu/ resedinta, amprenta digitala/ papilara, amprenta vocala, scan iris, date biometrice, ADN, amprenta vaselor de sange (daca exista), URL bloguri personale, pagini web personale, cod QR personal, inregistrari audio/ video (inclusiv supraveghere video interna si perimetru), inregistrari acces, venit (fluturasi salariu, extrase bancare), relatii de rudenie, adresa email, adresa IP, informatii privind traficul de Internet (adrese accesate, pagini vizualizate, click-uri), numar telefon, semnatura, varsta, sex, data nasterii, functie, istoric si evaluare profesionala, rezultate teste (e.g. medicale, auto) date privind proprietatile care pot identifica persoana (e.g. numar inmatriculare autovehicul, serie sasiu, numar cadastral locuinta), coordonate GPS

b) **aplicabilitatea teritoriala**: Regulamentul se aplica:
   - prelucrarilor efectuate de un operator sau imputernicit cu sediul in UE,
   - prelucrarilor de date personale ale unor persoane aflate in UE, efectuate de un operator sau imputernicit care nu e in UE (extinderea semnificativa a ariei geografice de aplicare a reglementarilor Uniunii Europene in domeniul datelor cu caracter personal), daca se ofera bunuri si servicii catre persoane aflate in UE (chiar daca nu este implicata o plata), se monitorizeaza comportamentul persoanelor din UE,

c) operatorii trebuie sa puna in aplicare **masuri tehnice** (e.g. IT si securitate fizica) **si organizatorice** (proceduri, coduri de conduit, interdictii, autorizari, verificari, permisiuni) adecvate pentru a indeplini cerintele Regulamentului si a proteja drepturile persoanelor vizate,

d) pentru a cunoaste ce (categorii de) date cu caracter personal detin si cu ce scop, organizatiile carora li se aplica Regulamentul trebuie sa realizeze o **cartografiere a datelor** cu caracter personal si a prelucrarilor efectuate asupra acestora (data mapping – evidenta activitatilor de prelucrare/ art 30), prin care sa identifice cel putin:
   - categoriile de persoane vizate,
   - categoriile de date cu caracter personal,
   - scopurile prelucrarii,
   - categoriile de destinatari,

---

si pentru abrogarea Legii nr 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date

- transferurile transfrontaliere de date,
- termenele limita pentru stergerea diferitelor categorii de date,
- masurile tehnice si organizatorice de securitate,

e) pentru prelucrarile susceptibile sa genereze un risc ridicat trebuie derulata o **analiza de impact** (DPIA – Data Protection Impact Analysis), analiza care implica:
   - consultarea prealabila a autoritatii de supraveghere,
   - descrierea procesului de prelucrare a datelor,
   - analiza principiilor de prelucrare a datelor,
   - identificarea si analiza riscurilor (inclusiv cu estimarea probabilitatii de producere si a impactului potential) si a potentialelor surse de risc,
   - implementarea masurilor de eliminare/ reducere a riscurilor,
   - consultarea cu DPO, persoanele vizate

f) standarde mai ridicate pentru obtinerea **consimtamantului**:
   - liber exprimat: neconditionat de prestarea serviciului, lipsa relatiei de subordonare,
   - specific si granular: exprimat pentru fiecare tip de prelucrare si scop al prelucrarii,
   - informat: existent unei informari adecvate si documentate,
   - neechivoc: identificare clara a obiectului consimtamantului,
   - actiune clara si pozitiva: tacerea sau abtinerea nu reprezinta un consimtamant,
   - documentat: existent unei evidente a exprimarii consimtamantului, pe suport hartie sau in format electronic,
   - retragerea consimtamantului trebuie realizata cu aceeasi usurinta ca si acordarea,

g) **transparenta** crescuta: necesitatea de a informa persoanele vizate (e.g. salariati, actionari, contractori) in privinta drepturilor de care beneficiaza, ceea ce implica elaborarea de proceduri si procese de informare si comunicare cu persoanele vizate, formulare de informare si o informare a personalului, actionarilor si partenerilor,

h) recunoasterea unor **drepturi noi** ale persoanelor vizate: informare, acces, rectificare, stergere, restrictionare, portabilitate, opozitie, decizii automate si profilare, restrictii,

i) necesitatea de a numi un **responsabil cu protectia datelor** cu caracter personal (DPO – Data Protection Officer), in anumite conditii de independenta si lipsa unui conflict de interese cu alte sarcini profesionale, cu necesitatea de a aloca resurse pentru activitatea acestuia (timp, echipamente, training, buget si accesul la date cu caracter personal si a operatiunilor de prelucrare aferente), si avand roluri specifice:
   - implicare efectiva in toate aspectele privind protectia datelor, inclusiv participarea cu regularitate la sedintele conducerii de nivel mediu/ superior, si asistenta/ implicare in cazul survenirii unui incident de securitate,
   - consilierea conducerii cu privire la obligatiile specifice si vulnerabilitatile identificate,
   - facilitarea/ coordonarea planurilor pentru implementare Regulament,
   - training pentru conducere si salariati privind obligatiile,
   - facilitarea radactarii documentatiei/ procedurilor pentru data mapping, evaluarea impactului asupra protectiei datelor (DPIA), proceduri interne de aplicare a Regulamentului,
   - punct de contact pentru persoanele vizate si autoritatea de supraveghere,
   - monitorizarea activitatilor organizatiei pentru facilitarea conformarii,

j) obligatia de a notifica imediat autoritatii de supraveghere cazurile de **incalcare a securitatii datelor** cu caracter personal si, in situatia unor riscuri ridicate privind datele cu caracter personal, si persoana vizata
   - incalcarea securitatii datelor cu caracter personal ("data breach"): incalcare a securitatii care duce, in mod accidental sau ilegal, la distrugerea, pierderea,

modificarea, sau divulgarea neautorizata a datelor cu caracter personal transmise, stocate sau prelucrate intr-un alt mod, sau la accesul neautorizat la acestea

k) Regulamentul solicita operatorilor sa demonstreze/ mentina o evidenta documentata in privinta modului de respectare a cerintelor Regulamentului, respectiv sa **documenteze conformarea** si modul de obtinere a asigurarii interne privind conformarea, ceea ce reprezinta o schimbare semnificativa a exercitarii autoritatii de catre autoritatea de supraveghere,

l) Revizuirea si modificarea cadrului de reglementare intern (proceduri, procese) care adreseaza date si prelucrari de date cu caracter personal,

m) **competente corective** ale autoritatii de supraveghere: Regulamentul ofera indicii privind gradatia aplicarii competentelor corective a operatorilor care nu se conformeaza cu prevederile Regulamentului (Regulamentul enumera competentele de la cele mai putin severe la cele mai severe), dar nu ofera siguranta aplicarii lor in ordinea in care sunt mentionate de Regulament. Competente corective: avertizari, mustrari, dispozitii, obligatii, limitari temporare sau definitive asupra prelucrarilor, retragerea unor certificari, impunerea de amenzi administrative (pana la 20 mil euro sau 4% din cifra de afaceri globala), suspendarea fluxurilor transfrontaliere de date.

3. Masuri implementate de SN Nuclearelectrica SA

Pentru conformarea cu cerintele Regulamentului, SNN SA a implementat un set de masuri tehnice si organizatorice si a intreprins actiuni de conformare si sau de implementare a cerintelor Regulamentului, astfel:

a) a fost numit un grup de lucru care sa realizeze analiza impactului noilor reglementari in organizarea si functionarea companiei si planul cu masurile ce trebuie implementate,

b) a fost realizata o prima analiza de impact a prevederilor Regulamentului, care a generat o identificare preliminara, pentru fiecare prevedere, a aplicabilitatii in privinta SNN, temeiul juridic, contextul si explicatii suplimentare pentru intelegerea si/sau aplicarea sa, precum si actiuni propuse si responsabili cu implementarea lor; o analiza similara a fost realizata in CNE Cernavoda cu referire la aspectele de resurse umane,

c) au fost identificate ariile si directiile de actiune (plan orientativ/ preliminar de actiune) pentru implementarea cerintelor Regulamentului,

d) a fost numit un responsabil cu protectia datelor (si notificat autoritatii de supraveghere), avand responsabilitatea de a informa si consilia conducerea si personalul SNN in privinta obligatiilor ce le revin in domeniul protectiei datelor si implementarii Regulamentului,

e) responsabilul cu protectia datelor a condus sesiuni de constientizare (awareness) si training pentru realizarea exercitiului de inventariere a prelucrarilor de date cu caracter personal (data mapping) cu compartimentele din Sediul Central si din sucursale,

f) a fost realizata o evidenta a activitatilor de prelucrare a datelor cu caracter personal (data mapping, conform art 30 din regulament), la care au participat toate structurile organizatorice din cadrul SNN,

g) au fost emise un set de proceduri interne care sa adreseze aspectele esentiale ale Regulamentului:
    a. Procedura generala de protectie a datelor cu caracter personal in SNN SA,
    b. Procedura de raspuns in caz de incalcare a securitatii datelor cu character personal,
    c. Prelucrarea datelor personale ale personalului SNN,
    d. Politica IT de prelucrare a datelor cu caracter personal in SNN SA,

h) a fost modificat website-ul SNN, fiind actualizat cu:
    a. Politica privind prelucrarea si protejarea datelor cu caracter personal in cadrul SNN,
    b. Informarea publicului privind prelucrarea datelor cu caracter personal in SNN SA, a drepturilor acestuia si a modurilor de exercitare a acestor drepturi,
    c. Informarea candidatilor la posturile scoase la concurs privind prelucrarea datelor cu caracter personal pe parcursul procesului de selectie, a drepturilor candidatilor si a modurilor de exercitare a acestor drepturi,
    d. Datele de contact ale responsabilului cu protectia datelor

i) au fost stabilite clauzele contractuale standard pentru actualizarea contractelor comerciale in care SNN este parte si a fost demarat procesul de semnare a actelor aditionale necesare,

j) au fost realizate formularele de informare catre salariati, parteneri contractuali, actionari, public si mass-media,

k) au fost realizate formulare de consimtamant pentru salariati si parteneri comerciali,

4. Actiuni viitoare

In urma intalnirilor derulate in perioada de implementare a pachetului esential de masuri a fost identificata o lista de actiuni necesar a fi implementate in continuare, acestea (sau variante modificate ale acestora in urma analizelor interne) urmand sa fie implementate treptat in perioada urmatoare.

Dintre acestea mentionam:

a) Numirea unui grup de lucru care sa coordoneze si sa sprijine, printr-o coordonare integrata si unitara (CNE Cernavoda-SNN Executiv-FCN) implementarea corecta si completa a cerintelor Regulamentului GDPR, cu emiterea de catre DG a unei Decizii in acest sens,

b) Extinderea/ detalierea analizei realizate in cadrul exercitiului de data mapping (evidenta datelor cu caracter personal si a prelucrarilor efectuate asupra acestora) pentru verificarea completitudinii considerarii tuturor departamentelor/ compartimentelor CNE Cernavoda care prelucreaza date cu caracter personal si procedurarea la nivelul departamentelor, prin intermediul IDP-urilor, a activitatii de prelucrare date cu caracter personal,

c) Identificarea, in urma extinderii/ detalierii analizei realizate in cadrul exercitiului de data mapping, a masurilor suplimentare necesar a fi implementate, daca va fi cazul,

d) Revizuirea treptata a cadrului de reglementare interna in scopul actualizarii reglementarilor interne pentru conformare cu cerintele Regulamentului,

e) Dezvoltarea unui program intern de comunicare interna, pregatire si constientizare a personalului SNN in privinta cerintelor Regulamentului,

f) Evaluarea independenta a gradului de conformare cu cerintele Regulamentului GDPR in toate unitatile SNN (recomandabil printr-o firma externa abilitata), dupa implementarea cu resurse interne.

…….
Ovidiu Bordeut
Responsabil cu protectia datelor
Serviciul Managementul Riscului, SNN Executiv