

Birou Dezvoltare Strategica
 Nr. 213/13.03.2018

Catre Consiliul de Administratie al Oil Terminal S.A.

Referitor adresa nr 100.931/08.03.2018 primita de la Cabinet Ministru- Ministerul Energiei privind Regulamentul UE 2016/679 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal.

Avand in vedere adresa susmentionata prin care se solicita ca in cadrul unei Adunari Generale, convocata pentru o data anterioara datei de 25.05.2018 (data de intrare in vigoare la nivelul UE a Regulamentului privind protectia datelor personale), societatea sa prezinte o informare privind masurile ce vor fi întreprinse pentru asigurarea protecției datelor cu caracter personal si pentru a minimiza riscul aplicarii unor sanctiuni, va supunem spre aprobare urmatorul plan de masuri:

Nr. Crt.	Masura	Responsabil	Termen de implementare	Observatii
1.	Declararea scopului si a mijloacelor prelucrării datelor cu caracter personal, care pot fi prin mijloace automate si/sau prin alte mijloace decat cele automate	-Conducerea executiva	31.03.2018	In Oil Terminal se opereaza date cu caracter personal ale: <ul style="list-style-type: none"> - Salariatilor si membrilor familiilor acestora - Actionarilor - Administratorilor - Clientilor - Furnizorilor - Persoanelor fizice care aplica pentru un loc de munca in cadrul societatii - Studentilor/practicantilor - Fostilor salariati si membrilor familiilor acestora
2.	Desemnarea unui responsabil cu protectia datelor si a inlocuitorului de drept prin decizia interna a conducerii societatii	-Conducerea executiva	31.03.2018	Acest responsabil cu protectia datelor va gestiona procesul de protectie a datelor cu caracter personal la nivelul societatii
3.	Identificarea si stabilirea utilizatorilor si mijloacelor de prelucrare a datelor cu caracter personal la nivelul societatii si nominalizarea lor prin decizie interna impreuna cu limitele de competenta si de autoritate	-Conducerea executiva	31.03.2018	
4	Transmiterea unei notificari catre Autoritatea Nationala de Supraveghere a Prelucrării Datelor cu Caracter Personal in vederea inregistrării ca operator de date cu caracter personal	-Conducerea executiva	30.04.2018	
5.	Instruirea, formarea si constientizarea responsabilului cu protectia datelor cu caracter personal, precum si a persoanelor responsabile cu prelucrarea datelor cu caracter personal la nivelul societatii privind scopul	-Conducerea executiva -Sef Serv RU -Sef structura functionala -Responsabil cu protectia datelor	30.04.2018	Este necesara instruirea si formarea profesionala, atat a responsabilului cu protectia datelor cu caracter personal, precum si a persoanelor responsabile cu prelucrarea datelor cu caracter personal la nivelul societatii printr-un Furnizor/Formator de instruire extern

	si mijloacele prelucrării datelor cu caracter personal si cerintele legislatiei specifice			specializat si autorizat pentru formarea personalului in acest domeniu
6.	Elaborarea unei/unor politici de securitate a prelucrării datelor cu caracter personal și a unei/ unor proceduri operationale care sa reglementeze activitatea, precum și măsurile organizatorice si tehnice de asigurarea securitatii protectiei prelucrării datelor cu caracter personal la nivelul societatii	-Conducerea executiva -Sef Birou Dezvoltare Strategica -Responsabil cu protectia datelor cu caracter personal -Compartiment Securitate Cibernetica	20.05.2018	Se va elabora, aviza si aproba o procedura operationala in conformitate cu cerintele Procedurii de sistem Realizarea procedurilor formalizate pe activitati si a Codului controlului intern managerial al entitatilor publice aprobat prin Ordinul nr.400/2015, cu modificarile si completarile ulterioare
7.	Implementarea si monitorizarea politicii de securitate a prelucrării datelor cu caracter personal și a procedurii/procedurilor operationale care sa reglementeze activitatea de prelucrare a datelor cu caracter personal la nivelul societatii	-Conducerea societatii -Sefi de structură functionala -Utilizatorii, salariatii din cadrul societatii care prelucreaza date cu caracter personal -Responsabil cu protectia datelor cu caracter personal	25.05.2018	
8.	Elaborarea/actualizarea fiselor de post, cu stabilirea și alocarea atribuțiilor și responsabilitatilor, precum si a limitelor de competenta aferente personalului care raspunde de gestionarea procesului de prelucrare si protectie a datelor cu caracter personal	-Conducerea societatii -Sefi de structură functionala -Sef Serv. RU	25.05.2018	
9.	Identificarea, analiza, evaluarea si gestionarea riscurilor aferente procesului de prelucrare si protectie a datelor cu caracter personal	-Conducerea societatii -Sefi de structură functionala -Sef Birou Dezvoltare Strategica -Sef Birou TIT -Compartiment Securitate Cibernetica -Responsabil cu protectia datelor cu caracter personal	25.05.2018	Se va aplica metodologia de lucru privind idetificarea, analiza, evaluare si gestionarea riscurilor implementată la nivelul societatii prin intermediul Procedurii de sistem Managementul riscului cod PS-02, Ed.I, R0.

Premise de ducere la indeplinire a masurilor propuse

- Conducerea societatii va intreprinde toate demersurile si va alocă toate resursele umane, materiale și financiare necesare pentru implementarea atat a acestui plan de masuri, cat si a cerintelor vizate de Regulamentul nr.679/ din 27 aprilie 2016 privind protecția 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).
- Prelucrarea datelor cu caracter personal trebuie realizata intr-un mod adecvat, legal, echitabil si transparent, atat fata de persoanele vizate, cat si in raport cu scopurile pentru care sunt prelucrate datele cu caracter personal în vederea asigurării securitatii adecvate a datelor cu caracter personal, inclusiv protectia impotriva prelucrării neautorizate sau ilegale sau impotriva pierderii, a distrugerii sau a deteriorării accidentale ori in scopul prevenirii

accesului sau utilizării neautorizate, prin luarea de măsuri tehnice și organizatorice corespunzătoare (integritate și confidențialitate).

- Prelucrarea datelor cu caracter personal se va face pe baza consințământului persoanelor vizate și/sau potrivit dispozițiilor legii și în raport cu scopurile pentru care sunt prelucrate datele.
- Nivelul de protecție și securitate a prelucrării datelor cu caracter personal se va consolida prin măsuri de protecție adecvate de asigurarea securității rețelelor informatice și a sistemelor informatice, cât și prin supravegherea și monitorizarea video și acces restricționat la nivelul spațiilor de păstrare a datelor cu caracter personal, prin elaborarea și implementarea de politici și proceduri de securitate a prelucrării datelor cu caracter personal și de securitate cibernetică, precum și măsuri specifice de control, cum ar fi afișarea și scrierea la loc vizibil cât și în zonele de acces a unor mesaje privind accesul controlat, postarea unor pictograme cu mesajul supraveghere video, etc.. De asemenea, se vor implementa metode de restricționare a accesului pe mai multe niveluri (multi-nivel) pentru categoriile speciale de date cu caracter personal, (ex: date privind starea de sănătate, datele genetice, chiar fotografiile, originile rasiale, etnie, religie, etc). Faptul că prelucrarea datelor cu caracter personal pentru categoriile speciale este restricționată va trebui să fie indicat în mod clar și în sistemul informatic prin avertizări ale sistemului de operare.
- Se vor elabora și implementa norme și documente care vor stabili reguli și responsabilități clare și precise privind protecția și prelucrarea datelor cu caracter personal la nivelul societății cu respectarea întocmai a cerințelor legale.
- Se vor stabili atribuții, responsabilități și răspunderi precise și clare, precum și limite de competență prin intermediul fișelor de post/decizii pentru toți utilizatorii autorizați care prelucrează date cu caracter personal la nivelul societății. Prin aceste măsuri, aceștia trebuie să fie informați și conștientizați de faptul că orice greșeală poate conduce la compromiterea reputației sau poate implica chiar răspunderea materială, civilă, contravențională sau penală, după caz.
- Se vor identifica, analiza, evalua și gestiona riscurile de securitate ale sistemului informatic actual la nivelul societății împreună cu Biroul Tehnologie Informației și Telecomunicații și Compartimentul Securitate Cibernetică și se vor gestiona prin intermediul registrului riscurilor, planului pentru implementarea măsurilor de control, strategiei de risc și metodologiei de risc aplicate.

Director General,
Sorin Viorel Ciutoreanu

Director Dezvoltare,
Marieta Stasi

Sef Birou Juridic-Litigii,
Mihaela Ignat

Sef Serviciu Resurse Umane,
Liliana Mihailov

Sef Birou Dezvoltare Strategica,
Constantin Pita

Specialist Strategie,
Victor Samoila