Roluri si responsabilitati în GDPR

Pentru societatea CLEAN RECYCLE S.A.

1. Introducere

Firma: **CLEAN RECYCLE S.A.**, tratează foarte serios securitatea datelor cu caracter personal pe care le colecteaza si le prelucrează în activitatea desfăsurată. Unul dintre atributele cheie ale unei abordări eficiente a protecției datelor este o repartizare clară a rolurilor în societate, fiecare persoană desemnată având responsabilități bine definite. Fiecare dintre aceste roluri trebuie alocat anumitor persoane sau grupuri din cadrul societatii/organizației.

Este vital ca tot personalul să înțeleagă rolul pe care trebuie să îl aibă în protecția datelor cu caracter personal și cum își va aduce contribuția.

2. Rolurile în Protecția Datelor

În cadrul normelor legale relevante pentru conformitatea cu GDPR, următoarele roluri majore trebuie definite și alocate:

- Operatorul de date;
- Persoana împuternicită;
- Managerul de Securitate informațională.

Responsabilitățile specifice ale fiecărui rol vor fi definite în secțiunile ulterioare ale acestui document.

Există, de asemenea, responsabilități particulare privind protecția datelor care trebuie efectuate de alte persoane ale societatii și care vor fi de asemenea explicate în acest document.

Aceste roluri sunt indeplinite de:

- Conducere;
- Sefii departamentelor;
- Angajati.

În general, responsabilitățile care se aplică tuturor angajaților, partenerilor comerciali și altor părți interesate sunt evidențiate în politicile organizaționale relevante ale societatii/organizației.

3. Responsabilități specifice rolurilor

Această secțiune detaliază responsabilitățile specifice de protecție a datelor pentru fiecare rol din structura societatii **CLEAN RECYCLE S.A.**

3.1. Operatorul de Date

Regulamentul GDPR definește „**operatorul**" ca fiind "*persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal*" (**articolul 4 pct. 7**). Responsabilitățile descries mai jos pot fi atribuite unei persoane individuale sau se aplica întregii organizații.

Operatorul de Date are următoarele responsabilități:

- Să se asigure că principiile referitoare la prelucrarea datelor cu caracter personal descrise la **articolul 5** din Regulamentul GDPR sunt respectate și este în măsură să demonstreze respectarea acestora. Pe scurt, Operatorul de Date trebuie să se asigure că datele cu caracter personal sunt:
    - Prelucrate în mod legal, corect și transparent;
    - Colectate în scopuri specifice, explicite și legitime;
    - Adecvate, relevante și limitate la ceea ce este necesar;
    - Exacte și dacă este necesar, actualizate;
    - Păstrate într-o formă care permite identificarea persoanelor vizate nu mai mult decât este necesar;
    - Prelucrate într-un mod care să asigure o securitate adecvată;
- Să se asigure că, în anumite cazuri, consimțământul persoanei vizate supuse prelucrării datelor cu caracter personal este obținut acolo unde este necesar, inclusiv consimțământul părinților pentru copii;
- Să furnizeze toate informațiile necesare în baza Regulamentului GDPR persoanei vizate într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, folosind un limbaj simplu și clar;
- Să faciliteze exercitarea drepturilor persoanelor vizate în temeiul Regulamentului GDPR si sa aiba un control cat mai bun asupra cererilor depuse de aceste persoane;
- Să implementeze măsuri tehnice și organizatorice adecvate pentru a se asigura și a fi capabil să demonstreze că prelucrarea este efectuată în conformitate cu Regulamentul GDPR;

- Să se asigure că alege doar acele persoane împuternicite care furnizează suficiente garanții privind implementarea unor măsuri tehnice și organizaționale adecvate în conformitate cu Regulamentul GDPR și care să asigure totodată protecția datelor personale;

- Să mențină o înregistrare a activităților de prelucrare a datelor cu caracter personal care intră în responsabilitatea persoanei împuternicite;

- Să coopereze, la cerere, cu Autoritatea de supraveghere în îndeplinirea sarcinilor sale;

- Să se asigure că orice persoană care acționează sub autoritatea persoanei împuternicite care are acces la datele cu caracter personal nu le procesează, cu excepția instrucțiunilor persoanei împuternicite;

- Să notifice o încălcare a datelor cu caracter personal Autorității de supraveghere, cu excepția cazului în care încălcarea nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice, în conformitate cu procedurile societatii;

- Să documenteze orice încălcare a datelor cu caracter personal, inclusiv faptele referitoare la încălcarea datelor cu caracter personal, efectele acestuia și măsurile de remediere luate;

- Dacă este cazul, să comunice persoanei vizate o notificare cu privire la încălcarea securității datelor cu caracter personal, fără întârzieri nejustificate;

- Să efectueze evaluări de impact privind protecția datelor, după caz, atunci când este obligatoriu;

- Să desemneze un responsabil cu protecția datelor atunci când este cerut de Regulamentul GDPR, si să publice detaliile acestuia și să le comunice Autorității de Supraveghere;

- Să sprijine responsabilul cu protecția datelor în îndeplinirea sarcinilor sale, oferind resursele necesare pentru îndeplinirea acestor sarcini și accesul la datele cu caracter personal și operațiunile de prelucrare;

- Să transfere datele cu caracter personal într-o țară terță sau într-o organizație internațională numai dacă operatorul sau persoana împuternicită a furnizat garanții adecvate și cu condiția ca drepturile aplicabile ale persoanelor vizate și căile de atac eficiente pentru persoanele vizate să fie disponibile;

3.2. Persoana împuternicită

Regulamentul GDPR definește "**persoana împuternicită**" ca fiind "*persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter*

personal în numele operatorului" (**articolul 4 pct. 8**). Responsabilitățile descrise mai jos pot fi atribuite unei persoane individuale sau se aplica întregii societati/organizații.

Persoana împuternicită are următoarele responsabilități:

- Să se asigure că orice prelucrare a datelor cu caracter personal este reglementată de un contract sau de un alt act juridic care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile persoanelor vizate și obligațiile și drepturile operatorului de date;

- Să proceseze datele cu caracter personal numai pe baza instrucțiunilor documentate ale operatorului de date, inclusiv în ceea ce privește transferul datelor cu caracter personal către o țară terță sau o organizație internațională;

- Se asigură că persoanele autorizate să proceseze datele cu caracter personal s-au angajat să păstreze confidențialitatea sau că au obligația legală de confidențialitate;

- Să implementeze măsurile tehnice și organizatorice adecvate pentru a asigura un nivel de securitate adecvat riscului asociat procesării neautorizate a datelor cu caracter personal;

- Să obțină autorizația anterioară specifica sau generala a operatorului de date înainte de a angaja o altă persoană împuternicită;

- Să asiste operatorul de date în îndeplinirea obligației operatorului de date de a răspunde cererilor de exercitare a drepturilor persoanei vizate;

- Să șteargă sau să returneze toate datele personale către operatorul de date după încetarea furnizării serviciilor legate de prelucrare;

- Să pună la dispoziția operatorului de date toate informațiile necesare pentru a demonstra conformitatea cu obligațiile stabilite în Regulamentul GDPR și să contribuie la audituri, inclusiv inspecțiile, efectuate de operatorul de date sau de un alt auditor mandatat de operatorul de date;

- Să mențină o înregistrare a tuturor categoriilor de activități de prelucrare efectuate în numele unui operator de date;

- Să coopereze, la cerere, cu Autoritatea de supraveghere în îndeplinirea sarcinilor sale;

- Să se asigure că orice persoană care acționează sub autoritatea persoanei împuternicite care are acces la datele cu caracter personal nu le procesează decât pe baza instrucțiunilor Operatorului de date;

- Să notifice operatorul de date fără întârzieri nejustificate după ce a constatat o încălcare a datelor cu caracter personal;

- Să desemneze un responsabil de protecție a datelor atunci când este cerut de Regulamentul GDPR, să publice detaliile acestuia și să le comunice Autorității de Supraveghere (atunci cand este necesar) ;

- Să sprijine responsabilul cu protecția datelor în îndeplinirea sarcinilor sale, oferind resursele necesare pentru îndeplinirea acestor sarcini și accesul la datele cu caracter personal și operațiunile de prelucrare (in cazul in care este nevoie sa fie desemnat DPO);

3.3 Sef departament Securitate Informațională

Managerul de Securitate Informațională este actorul principal pe aspecte de securitate și probleme conexe.

Managerul de Securitate Informațională are următoarele responsabilități:

- Raportarea către conducere a tuturor aspectelor legate de securitate, atât în mod regulat, cât și ad-hoc atunci când este necesar;

- Să comunice politica de securitate a informațiilor tuturor părților interesate relevante, inclusiv clienților, după caz;

- Să implementeze cerințele politicii de securitatea informațiilor;

- Să managerizeze riscul asociat cu accesul la servicii sau sisteme;

- Să se asigure că există controale de securitate și că acestea sunt documentate;

- Să cuantifice și să monitorizeze tipurile, volumele și impactul incidentelor de securitate;

- Să definească planuri de îmbunătățire și targeturi pentru anul financiar urmator;

- Să faca monitorizarea acestor targeturi;

- Să identifice și să reduca incidentele de securitate privind informațiile în conformitate cu o procedură bine stabilită;

4. Alte roluri în legătură cu responsabilitatea protecției datelor

Există o serie de alte roluri interne în cadrul societatii/ organizației care, deși nu sunt dedicate exclusiv protecției datelor, au responsabilități conexe cu acest domeniu.

4.1. Managerii de Departament

Managerii de Departament pot fi șefii sau supervizorii unităților operaționale din cadrul societatii.

Un Manager de Departament are umătoarele responsabilități din punct de vedere al Regulamentului GDPR:
Să revizuiască și să conducă nevoile și competențele angajaților astfel încât să le permita să își îndeplinească sarcinile în mod eficient în cadrul protecției datelor cu caracter personal;
Să se asigure că angajații sunt conștienți de relevanța și importanța activităților acestora și de modul în care contribuie la atingerea obiectivelor privind protejarea datelor personale;
Să participe și să contribuie la realizarea analizei impactului privind protecția datelor care afectează domeniul lor de activitate.

4.2 Angajații

Responsabilitățile tuturor angajaților sunt definite într-o varietate de politici la nivelul întregii societati/ organizații și sunt prezentate doar pe scurt în cele ce urmează.
Un angajat are următoarele răspunderi principale:
Se asigură că sunt constienți de toate politicile privind protecția datelor la nivelul societatii/organizației în legătură cu rolul pe care îl dețin;
Să anunțe orice fel de încălcare actuală sau potențială de securitate a datelor personale.

Firma: CLEAN RECYCLE S.A.
Administrator: Monda Radu Cosmin

SOCIETATEA CLEAN RECYCLE S.A. 2 BUCUREȘTI - ROMANIA