PROCEDURA OPERAȚIONALĂ DE RAPORTARE ȘI TRATARE A INCIDENTELOR DE SECURITATE

Cod: PO-10

Cuprins

2. Scopul procedurii

2.1. Prezenta procedură documentează cerințele GDPR privind procedura de raportare și tratare a incidentelor de securitate și are rolul de a prezenta modalitatea concretă de notificare a Autorității de Supraveghere privind Protecția Datelor cu Caracter Personal și de informare a persoanei vizate în cazul în care se produce o încălcare a securității datelor cu caracter personal.

2.2. Prezenta procedură descrie activitățile desfășurate atunci când se produce un incident de securitate, respectiv, înregistrarea încălcărilor de securitate, întocmirea notificărilor și informărilor impuse de GDPR, stabilirea fluxului de parcurs în redactarea și difuzarea controlată a acestora către Autoritatea de Supraveghere și persoanele vizate.

2.3. Prin această procedură se urmărește asigurarea unui flux corect, eficient și legal al notificărilor transmise către Autoritatea de Supraveghere și al informărilor persoanelor vizate în cazul încălcării securității datelor cu caracter personal, în temeiul GDPR și al legislației conexe.

2.4. GDPR introduce o obligație pentru toate organizațiile de a raporta anumite tipuri de încălcare a securității datelor cu caracter personal către autoritatea de supraveghere – ANSPDCP, în termen de 72 de ore de la constatarea încălcării. Dacă este depășit acest termen, trebuie furnizate motive temeinice pentru întârziere.

2.5. GDPR introduce obligația informării persoanelor vizate cu privire la încălcarea securității datelor cu caracter personal dacă încălcarea respectivă este susceptibilă să genereze un risc ridicat de afectare negativă a drepturilor și libertăților persoanelor vizate, fără întârzieri nejustificate.

3. Domeniul de aplicare

Prezenta procedură se aplică tuturor structurilor organizatorice ale companiilor GreenGroup. Procedura este întocmită în scopul pregătirii pentru producerea unei încălcări a securității datelor cu caracter personal și planul de reacție la aceasta, precum și a atribuțiilor persoanelor implicate în procesul de notificare a Autorității de Supraveghere și de informare a persoanelor vizate afectate. La procedură participă toate structurile organizatorice conform cu atribuțiile care le revin în ceea ce privește asigurarea securității datelor cu caracter personal.

4. Documente de referință

- Regulament Intern al **companiilor GreenGroup**

- Politica generală internă privind protecția datelor cu caracter personal

5. Definiții și abrevieri

5.1.Definiții ale termenilor

5.1.1. Autoritate de supraveghere - autoritate publică independentă instituită de un stat membru cu atribuții în materia protecției datelor cu caracter personal.

5.1.2. Consimțământ – al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

5.1.3. Date cu caracter personal – orice informații privind o persoană fizică identificată sau identificabilă („persoană vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

5.1.4. Destinatar - persoană fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării.

5.1.5. Încălcarea securității datelor cu caracter personal - 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.

5.1.6. Operator - 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; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern.

5.1.7. Parte terță - persoana fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub

directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal.

5.1.8. Persoana împuternicită de operator - persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului.

5.1.9. Prelucrare - orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

5.1.10. Regulament GDPR - Regulamentul (UE) 2016/679 al Parlamentului Eurpean 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.

5.1.11. Reguli corporatiste obligatorii - politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoana împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună.

5.1.12. Reprezentant - persoana fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul GDPR.

5.2.Abrevieri ale termenilor

ANSPDCP	Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
DC	Director Calitate
DPIA	Evaluarea impactului asupra protecției datelor (în limba engleză, data-protection impact assessment)
DPO	Responsabilul cu protecția datelor (în limba engleză, data protection officer)
ESG	Environmental, Social, Governance (Mediu, Social, Guvernanță)

GDPR	Regulamentul general privind protecția datelor (în limba engleză General Data Protection Regulation)
HR	Resurse Umane

6. Descrierea procedurii

6.1.Aspecte generale

Incidentul de securitate înseamnă o încălcare a securității care duce la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal, în mod accidental sau ilegal. Aceasta include încălcările cauzate atât în mod accidental, cât și în mod intenționat.

Încălcările de securitate vor fi raportate la ANSPDCP fără întârzieri nejustificate, în cel mult 72 de ore de la constatarea acesteia. În măsura în care nu este posibilă furnizarea tuturor informațiilor în termenul menționat, acestea vor fi transmise etapizat. În orice situație de depășire a termenului de 72 de ore de la constatarea încălcării, vor fi furnizate motive pentru întârziere, precum și termenul preconizat în interiorul căruia vor fi transmise mai multe informații.

În cazul în care încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor vizate, vor fi informate persoanele în cauză în mod direct și fără întârzieri nejustificate, cât mai repede posibil.

În momentul producerii unei încălcări a securității datelor cu caracter personal, orice informații care se furnizează ANSPDCP sau persoanei vizate vor fi concise, ușor accesibile și ușor de înțeles și să utilizeze un limbaj simplu și clar, precum și elemente grafice acolo unde este cazul.

6.2. Descrierea încălcărilor

Încălcarea securității datelor cu caracter personal poate afecta confidențialitatea, integritatea sau disponibilitatea datelor cu caracter personal.

Încălcările securității datelor cu caracter personal pot cuprinde:

- accesul unui terț neautorizat;
- acțiunea (sau inacțiunea) intenționată sau accidentală a unui operator sau unei persoane împuternicite de operator;

- trimiterea unor date cu caracter personal către un destinatar greșit;
- pierderea sau furtul unor dispozitive informatice care conțin date cu caracter personal;
- modificarea datelor cu caracter personal fără permisiune;
- pierderea disponibilității datelor cu caracter personal.

6.3. Înregistrarea încălcărilor de securitate

Persoana responsabilă de înregistrarea incidentelor cu privire la încălcarea securității datelor cu caracter personal este: Bratu Daniel (DPO).

DPO-ul are următoarele sarcini:

- ✓ primește informările cu privire la incidentele de securitate;
- ✓ conlucrează cu celelalte departamente în vederea analizării incidentului de securitate;
- ✓ înregistrează incidentele de securitate în Registrul de evidență [**Registrul privind încălcările securității datelor cu caracter personal**];
- ✓ răspunde de menținerea Registrului de evidență.

Reguli generale privind înregistrarea:

a) toate documentele care privesc aceeași problemă se conexează la primul act înregistrat, numărul primului act fiind numărul de bază;

b) actele transmise se înregistrează cronologic, începând cu data de 1 ianuarie și terminând cu data de 31 decembrie a fiecărui an; actele care sunt transmise de către societate prin poștă sau curieri se înregistrează în ordinea transmiterii lor;

c) atât documentele care se înregistrează, cât și răspunsurile și actele transmise către Autoritatea de Supraveghere și/sau persoanele vizate vor purta numărul de înregistrare al documentului;

d) este interzisă circulația în cadrul societății companiilor GreenGroup a documentelor cu privire la încălcarea securității datelor cu caracter personal care nu sunt înregistrate.

6.4.Analiza încălcărilor de securitate

Unele încălcări a securității datelor cu caracter personal nu vor conduce la riscuri ce depășesc posibilele inconveniente pentru persoanele care au nevoie de datele respective pentru munca lor. Alte încălcări pot afecta în mod semnificativ persoanele ale căror date cu caracter personal au fost compromise.

În analiza incidentelor de securitate se vor avea în vedere următoarele aspecte:

- ✓ prejudicii de natură fizică, materială sau morală a persoanelor fizice, cum ar fi pierderea controlului asupra propriilor date cu caracter personal, limitarea propriilor drepturi,

discriminarea, furtul sau frauda identității, pierderea financiară, inversarea neautorizată a pseudonimizării;

- ✓ compromiterea reputației societății;
- ✓ pierderea confidentialității datelor cu caracter personal protejate prin secret profesional;
- ✓ orice alt dezavantaj semnificativ de natura economică sau socială pentru persoana fizică vizată.

În vederea analizării acestora, persoana responsabilă (DPO) va obține informații de la șefii de departamente / compartimente.

Persoanele din cadrul departamentelor companiilor GreenGroup care întocmesc documente și transmit informații despre persoanele vizate poartă întreaga răspundere asupra datelor și conținutului acestora, iar în cazul transmiterii unor date sau informații eronate, vor răspunde potrivit reglementărilor în vigoare.

Persoana responsabilă de înregistrarea încălcărilor va consemna următoarele elemente:

- descrierea situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal;
- efectele produse;
- masurile de remediere întreprinse.

6.5. Evaluarea gravității impactului posibil sau efectiv

În evaluarea riscului pentru drepturile și libertățile persoanelor vizate, se va pune accentul pe posibilele consecințe negative și vor fi indicate elemente din care să rezulte probabilitatea materializării și gravitatea riscului rezultat ca urmare a incidentului produs. Dacă există probabilitatea ca un risc să se materializeze, atunci trebuie notificată ANSPDCP; dacă nu există această probabilitate, atunci nu trebuie raportată încălcarea.

Societatea păstrează documente referitoare la toate incidentele de securitate, chiar dacă nu există obligația de raportare către Autoritate sau nu prezintă un risc ridicat pentru persoanele vizate.

Persoana responsabilă cu evaluarea gravității impactului este Bratu Daniel (DPO-ul societății). În urma evaluării gravității impactului, persoana responsabilă, în raport de toți factorii relevanți, va completa un raport care se înaintează Directorului General al GreenTech S.A.

6.6. Notificarea către Autoritatea de Supraveghere

În cadrul societății se transmit notificări cu privire la încălcarea securității datelor cu caracter personal prin următoarele mijloace:

- e-mail: protectia.datelor@green-group.ro
- alte modalități: telefonic, la 0730230807 (DPO)

În momentul raportării unei încălcări, trebuie incluse următoarele informații:

- ✓ descrierea caracterului încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- ✓ numele și datele de contact ale responsabilului cu protecția datelorcompaniilor GreenGroup sau un alt punct de contact de unde se pot obține mai multe informații;
- ✓ descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
- ✓ descrierea măsurilor luate sau propuse spre a fi luate pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile luate pentru atenuarea eventualelor efecte negative.

Pentru transmiterea Notificării către Autoritatea de Supraveghere se va folosi modelul pus la dispoziție [**Formular de notificare a încălcării securității datelor către ANSPDCP –** *Anexa 1*].

Persoana responsabilă de transmiterea Notificării către Autoritatea de Supraveghere este Bratu Daniel (responsabil de protecția datelor cu caracter personal). Termenul de transmitere a notificării este 72 de ore. Dacă este depășit acest termen, trebuie furnizate motive temeinice pentru întârziere.

6.7. Informarea persoanei vizate la solicitarea Autorității de Supraveghere

Persoana responsabilă de analiza solicitării primite din partea Autorității de Supraveghere cu privire la informarea persoanelor vizate este: Bratu Daniel (responsabil de protecția datelor cu caracter personal).

În cadrul societății se transmit informări cu privire la încălcarea securității datelor cu caracter personal prin următoarele mijloace:

- e-mail: protectia.datelor@green-group.ro
- alte modalități: telefonic la 0730230807 (DPO)

Persoanele vizate vor fi informate în următoarele situații:

- ✓ în cazul în care încălcarea este susceptibilă să genereze un risc ridicat (pragul pentru informarea persoanelor vizate este mai ridicat decât cel pentru notificarea ANSPDCP) pentru drepturile și libertățile persoanelor vizate, în mod direct și fără întârzieri nejustificate;
- ✓ gravitatea impactului posibil sau efectiv al unei încălcări asupra persoanelor vizate, cât și probabilitatea materializării sale este mare.

În măsura în care decizia este de a nu informa persoanele vizate, trebuie notificată ANSPDCP, dacă nu se poate demonstra că încălcarea nu este susceptibilă să genereze un risc pentru drepturi și libertăți. În orice caz, trebuie păstrate documente cu privire la procesul de luare a deciziei în conformitate cu cerințele principiului responsabilității.

Informarea către persoanele vizate va descrie, într-un limbaj clar și simplu, caracterul încălcării securității datelor cu caracter personal și va cuprinde următoarele informații:

- ✓ numele și datele de contact ale responsabilului cu protecția datelor din cadrul companiilor GreenGroup sau un alt punct de contact de unde se pot obține mai multe informații;
- ✓ descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;
- ✓ descrierea măsurilor luate sau propuse spre a fi luate pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile luate pentru atenuarea eventualelor efecte negative.

Informarea persoanei vizate **nu este necesară** în cazul în care:

a) s-au implementat măsuri de protecție tehnice și organizatorice adecvate în cazul datelor cu caracter personal afectate de încălcarea securității;

b) au fost luate măsuri de natură a conferi siguranța că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai este susceptibil să se materializeze;

c) ar necesita un efort disproporționat, caz în care se va efectua o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod eficace.

Persoana responsabilă de transmiterea Informării către persoana vizată este Bratu Daniel (DPO). Termenul de transmitere a Informării este de 72 de ore. Dacă este depășit acest termen, trebuie furnizate motive temeinice pentru întârziere.

6.8. Persoanele împuternicite de operator

Dacă societatea utilizează una sau mai multe persoane împuternicite, iar acestea suferă o încălcare de securitate, vor trebui să informeze operatorul fără întârzieri nejustificate, de îndată ce constată încălcarea pentru a lua măsuri în vederea tratării încălcării și a-și îndeplini

obligațiile de raportare a încălcărilor conform GDPR. Cerințele privind raportarea încălcărilor trebuie să fie detaliate în contractul încheiat cu persoana împuternicită, conform art. 28 GDPR.

6.9.Taxe

În cadrul societății companiilor GreenGroup informațiile furnizate persoanei vizate și orice comunicare sunt oferite în mod gratuit. În cazul în care cererile din partea unei persoane vizate sunt în mod vădit nefondate sau excesive (în special din cauza caracterului lor repetitiv), se va proceda la:

a) perceperea unei taxe, având în vedere costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;
b) refuzul de a da curs solicitării.

6.10.Semnare

Toate documentele întocmite cu privire la raportarea și tratarea incidentelor de securitate pentru a fi transmise în exteriorul companiilor GreenGroupvor fi semnate de către Bratu Daniel (DPO).

6.11. Închidere

Înainte de închiderea analizei incidentelor de securitate se va investiga dacă încălcarea a fost rezultatul unei erori umane sau al unei probleme sistematice și vor fi analizate măsuri pentru a preveni reapariția - fie prin procese mai bune, fie prin instruire suplimentară, fie prin alte măsuri corective.

După rezolvarea lor, toate actele cu privire la raportarea și tratarea incidentelor de securitate se grupează în bibliorafturi și se predau la arhivă în termen de 30 de zile. Predarea la arhivă se face pe bază de inventare (opis) întocmite în trei exemplare (un exemplar pentru cel care predă, un exemplar pentru dosarul din arhiva și un exemplar pentru dosarul de evidență a departamentului).

7. Formulare

Registrul incidentelor GDPR F1/PO-10

Model F1/PO-10

Incident	Data producerii	Data constatării	Datele cu caracter personal afectate	Persoanele vizate	Data notificării	Data notificării ANSPDCP	Motivul pentru care ANSPDCP nu a fost notificată

F1/PO-10, Ed.1

8. Anexe

Anexa	Conținut	Nr.pag.
Anexa 1	Notificare pentru încălcarea securității datelor cu caracter personal	6