S.C. ELECTRO GEAD SRL

Sediul : ***Str. Moise Nicoara nr. 41 , Bl. D3 , Sc. B , Et. 1 , Ap. 49 , Sector 3 , Bucuresti***

IRC : J40/7766/2004

CUI : RO16422281

POLITICA INTERNA PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

Referinta: ***General Data Protection Regulation***, *Regulamentul 2016/679 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 (GDPR)*

Legea 677/21.11.2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date, cu modificarile ulterioare

Intra in vigoare la : 25 mai 2018

Prelucrare de date: 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.

Prelucrarea datelor cu caracter personal: orice gen de activitate care este realizată cu și asupra acelor date, de la momentul colectării lor (inclusiv) și până la momentul distrugerii lor (inclusiv).

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, cum ar fi:

numele;
domiciliul sau reședința;
o adresă de e-mail (inclusiv adresele de tipul prenume.nume@firma.ro);
numărul de buletin, pașaport sau carte de identitate;
date privind locația (de exemplu, funcția de date privind locația disponibilă pe un telefon mobil);
un IP;
un cookie ID;
silueta cuiva din înregistrările CCTV;
un număr de înmatriculare al unei mașini;

Categoriile speciale de date cu caracter personal: sunt acelea care dezvăluie (conform art. 9 GDPR):
- originea rasială sau etnică;
- opiniile politice;
- confesiunea religioasă sau convingerile filozofice;
- apartenența la sindicate;
- date genetice;
- date biometrice pentru identificarea unică a unei persoane fizice;
- date privind sănătatea;
- privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

Operator: potrivit GDPR, prin „operator" se înțelege o persoană 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.

Împuternicit: „Persoană împuternicită de operator" înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism **care prelucrează datele cu caracter personal în numele operatorului**.

Există două condiții esențiale pentru ca o entitate să se califice drept împuternicit:
- Să fie entitate juridică separată față de operator; și

● Să prelucreze date în numele operatorului; această activitate de prelucrare poate fi limitată la o activitate foarte specifică sau poate fi mai generală și mai extinsă.

Împuternicitul este **instrumentul prin care Operatorul își realizează scopurile prelucrării**.

Calificarea contabililor poate varia în funcție de context. În cazul în care contabilii oferă servicii publicului general și micilor comercianți pe baza unor instrucțiuni foarte generale („pregătiți declarațiile mele de venit”), aceștia – la fel ca avocații care acționează în circumstanțe similare și din motive similare – vor avea rolul de operatori de date.

In situatia in care, cabinetul de contabilitate presteaza servicii financiar-contabile unui client, pe baza de contract de prestari servicii, cabinetul va avea rolul de persoană împuternicită, având în vedere instrucțiunile clare ale clientului și libertatea sa limitată de acțiune.

Atunci când profesionistii contabilii consideră că au detectat practici ilegale pe care sunt obligați să le raporteze, având în vedere obligațiile lor profesionale, aceștia acționează independent în calitate de operatori.

”O companie își externalizează serviciile de contabilitate. Atunci când acționează în numele clientului său care si-a externalizat serviciile de contabilitate, cabinetul de contabilitate este operator, din perspectiva datelor personale cuprinse în registrele contabile. Acest lucru se întâmplă pentru că un contabil ori alt furnizor profesional de servicii acționează in baza unor obligații profesionale ce le impun să își asume responsabilitatea pentru datele personale pe care le prelucrează. Spre exemplu, dacă un contabil detectează activități ilegale în timpul activității sale, poate fi obligat să raporteze aceste activități către poliție ori alte autorități. Prin realizarea acestui lucru, contabilul în cauză nu acționează în baza unor instrucțiuni primite de la client, ci în concordanță cu obligațiile profesionale pe care le are, deci devine, prin urmare, operator pe acel tip de prelucrări.

Persoana Vizată: acea persoană fizică in viata, ale cărei date sunt prelucrate.

Scopul prelucrării:
Calcularea si plata salariilor
Transmiterea Registrului general de evidenta a salariatilor
Întocmirea dosarului de salariat
Intocmirea contractelor comerciale, a facturilor si altor documente comerciale
Efectuarea operatiunilor de incasari/plati in numerar sau virament
Intocmirea de raportari in conformitate cu legislatia specifica

In cazul în care datele cu caracter personal sunt prelucrate într-un alt scop decât cel pentru care acestea au fost colectate, va trebui să se furnizeze persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și alte informații necesare.

Datele personale ce urmează sa fie prelucrate:

- elementele de identificare ale tuturor salariaților: numele, prenumele, codul numeric personal - CNP, cetățenia și țara de proveniență, adresa sau resedinta

- funcția/ocupația,

- datele din actele de studii de lungă durată ale persoanei, precum și

- datele privitoare la profilul/specializarea/calificarea, conform actelor/certificatelor de calificare,

- salariul de bază lunar brut și sporurile, astfel cum sunt prevăzute în contractul individual de muncă,

- adresa de e-mail, numar de telefon,

- datele personale ale membrilor de familie sau persoanelor aflate in intretinerea salariatului, daca este cazul,

Operațiunile de prelucrare:

- verificarea unui profil de pe platformele de comunicare socială, in situatia in care profilul candidatului de pe respectivele platforme este legat de un context profesional sau personal iar verificarea este necesara și relevantă pentru îndeplinirea atribuțiilor postului pentru care aceștia s-au înscris.
- Intocmirea statelor de plata, adeverinte, raportari, alte documente de personal-salarizare conform legii
- Intocmirea de contracte comerciale, facturi, etc.
- Intocmirea de ordine de plata / dispozitii de plata in numerar
- Intocmirea de raportari fiscale

Persoanele vizate în operațiunile de prelucrare pe care le implică muncă unui contabil, expert contabil sau auditor financiar sunt reprezentate de angajații potențiali sau actuali ai unei companii, precum și clientii acelei companii. Într-o mai mică măsură, prelucrarea datelor de către contabil sau auditorul financiar implică și administratorul, acționarii sau asociații unor companii.

Temeiul legal al operațiunii de prelucrare

Potrivit GDPR (art. 6 alin (1)), prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:
(a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
(b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
(d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

(e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;
(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Perioada de păstrare a datelor cu caracter personal și pe ce se fundamentează stabilirea acesteia

Datele cu caracter personal sunt **păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele;**
Documentele financiar-contabile care se păstrează timp de 5 ani, cu începere de la data încheierii exercițiului financiar în cursul căruia au fost întocmite: notă de recepție și constatare de diferențe, bon de consum, fișă de magazie, listă de inventariere, chitanță, dispoziție de plată/încasare către casierie, borderou de achiziție, borderou de achiziție (de la producători individuali), ordin de deplasare (delegație), ordin de deplasare (delegație) în străinătate (transporturi internaționale), decont de cheltuieli (pentru deplasări externe), decizie de imputare, etc.
Registrele de contabilitate obligatorii şi documentele justificative care stau la baza înregistrărilor în contabilitatea financiară se păstrează în arhiva timp de 10 ani, cu începere de la data încheierii exerciţiului financiar în cursul căruia au fost întocmite, cu excepţia statelor de salarii, care se păstrează timp de 50 de ani".

Măsurile de securitate care asigură o diminuare a riscului asupra drepturilor și libertăților persoanelor vizate (protectie impotriva prelucrarii neautorizate,, pierderii, distrugerii, deteriorarii accidentale, etc.)

- training-ul personalului intern;
- politici interne de securitate ;
- asigurarea accesului în clădire/birou/camere/dulapuri doar pentru persoanele care au dreptul să fie acolo;
- accesarea mijloacelor electronice de prelucrare a datelor, pe baza de parola

Principii de prelucrare a datelor cu caracter personal, conform GDPR

Datele cu caracter personal sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență");
● datele nu se utilizezaza în moduri care au efecte negative nejustificate asupra persoanelor în cauză;

● se ofera persoanelor respective o informare detaliată în momentul colectării datelor lor personale, cu privire la modul in care vor fi utilizate acestea.

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri („limitări legate de scop”);
● se ofera persoanelor vizate, în informarea prezentată la momentul colectării datelor lor personale, o trecere în revistă a scopurilor pentru care se colecteaza fiecare categorie de date;

● nu se schimba scopul pentru care au fost colectate datele, fără informarea prealabilă a persoanelor vizate

(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);
● se colecteaza un număr de date nici mai mic și nici mai mare pentru atingerea scopului propus, la momentul la care acestea sunt necesare;

(d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate”);

(e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele („limitări legate de stocare”), drept pentru care:
● stocarea datelor se face pentru perioada strict necesara prelucrarii sau impusa de lege.

(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”).

● măsuri tehnice și organizatorice necesare pentru a defini un grad sporit de securitate a prelucrării datelor, desemnarea unui responsabil si instruirea salariatilor.

Care sunt drepturile persoanelor vizate și ce implicații au aceste drepturi asupra companiei?
Privit ca ansamblu de reguli referitoare la protecția datelor cu caracter personal, GDPR pune în centrul său drepturile și libertățile persoanelor vizate. Pentru ca aceste drepturi și libertăți să fie respectate, Regulamentul obligă organizațiile (companii, autorități publice etc.) să aplice o serie de proceduri birocratice de natură să le determine să înțeleagă și să poată răspunde în timp util solicitărilor primite de la persoanele vizate ori de la Autoritățile de Supraveghere.
Avand în vedere că nu amenzile ar trebui să producă panică, ci realitatea dură, când persoanele vizate vor utiliza drepturile pe care le au pentru **a solicita accesul, ștergerea ori rectificarea datelor lor**, urmând ca, la aceste solicitări, să se dea un răspuns într-un termen impus de GDPR. Dacă estimăm numărul cererilor și asociem această realitate cu faptul că,

datele pot fi răspândite între mai multe baze de date, sisteme de referință sau metode de stocare, putem aprecia adevărata imagine a provocărilor GDPR.

Potrivit art. 12 din GDPR, compania în calitate de operator furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul articolelor 15-22 (dreptul de acces la date, dreptul de ștergere a datelor, dreptul la rectificarea datelor, dreptul de restricționare a datelor, dreptul la opoziție, dreptul la portabilitatea datelor), fără întârzieri nejustificate și în orice caz **în cel mult o lună de la primirea cererii.**
Această perioadă **poate fi prelungită cu două luni** atunci când este necesar, dar operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii.

E foarte important, însă, ca persoana vizată să fie identificată corect înainte de a i se furniza răspunsul la cererile sale. Identificarea trebuie să aibă în vedere, atunci când e cazul, inclusiv solicitarea de informații suplimentare, menite să ajute operatorul să identifice persoana vizată în sistemul său de referință.

Cererile formulate de persoanele vizate **nu trebuie să aibă o formă standard,** nu trebuie să fie completate folosind un șablon ori un tipizat. Ele pot veni pe orice fel de canal (verbal, electronic, prin telefon, poștă scrisă, facebook, messenger), în orice formă ar fi ele formulate (în limbaj obișnuit, în limbaj academic, juridic etc.).

GDPR nu conține prevederi speciale în acest sens. La alin (3) al art. 12, GDPR menționează doar că "În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format".
Răspunsul la astfel de cereri trebuie formulat folosind o metodă care să poată fi probată ulterior. Cu alte cuvinte, trebuie **formulat în scris (inclusiv în formă electronică) și trebuie inclus într-o bază**
sistematizată de răspunsuri, pentru a putea fi regăsit mai ușor în viitor, atunci când va fi nevoie de acest lucru.

Informarea persoanei vizate
Înainte de orice activitate de prelucrare (există și unele excepții), persoana vizată trebuie informată asupra activității respective. Informarea este obligatorie (e un drept al persoanei vizate) și trebuie să conțină o serie de puncte importante prevăzute în GDPR (art. 13 și 14).
Informarea trebuie realizată indiferent de temeiul utilizat pentru realizarea prelucrării (obligație legală, contract, interes legitim sau consimțământ, ca să le enumerăm pe cele care credem că se potrivesc în acest context).
Informarea trebuie să conțină punctele prezentate mai jos, în funcție de modul în care au fost obținute datele cu caracter personal. Datele sunt obținute, de regulă, direct de la persoana vizată (contract de muncă, CV etc). Există, însă, și situații în care datele sunt obținute indirect (ex. atunci când compania X cumpără compania Y și odată cu această achiziție are acces la baza cu clienți și angajați ai companiei Y).

De asemenea, foarte important este faptul că această informare trebuie realizată de către operator. Cu alte cuvinte, operatorul este cel care răspunde la întrebările de mai jos. Împuternicitul realizează prelucrările Operatorului. Prin urmare, el nu va trebui sa informeze persoana vizată asupra faptului că îi prelucrează datele, pentru că operatorul este cel obligat să o facă. Bineînțeles, operatorul ar trebui să amintească în informare că datele vor fi transferate și către împuterniciții săi în vederea furnizării unor servicii externalizate de contabilitate, salarizare, recrutare personal etc.

Drepturilor persoanelor vizate:

Dreptul la informare

Acesta le permite persoanelor vizate să știe, chiar de la momentul la care se face colectarea (sau în maximum o lună de la dobândirea datelor, în cazul datelor colectate indirect de la persoana vizată) modul în care se vor utiliza acele date, către cine vor fi ele dezvăluite ori transferate, ce drepturi au persoanele în cauză cu privire la datele prelucrate etc.

Dreptul de acces la date

Art. 15 GDPR permite persoanelor vizate să obțină, din partea operatorului, o confirmare că se prelucrează sau nu date cu caracter personal care le privesc și, în caz afirmativ, acces la datele respective și la alte informații utile.

Ca urmare a dreptului de acces, persoana vizată va primi o informare personalizată (vezi conținutul informării, așa cum e prezentat într-un capitol următor), de natură să îi explice ce date îi sunt prelucrate, în ce scop, în ce temei, care e perioada de retenție a acelor date, către cine pot fi ele transferate și în ce scop, menționarea drepturilor pe care le are persoana vizată cu privire la acele drepturi, inclusiv dreptul de a depune o plângere la Autoritatea de Supraveghere, dacă persoana nu e mulțumită de modul în care se redactează acest răspuns etc. În plus față de această informare cu privire la datele prelucrate, persoana vizată are dreptul de a obține o copie a datelor în cauză.

Dreptul la ștergerea datelor

Art. 17 GDPR permite persoanelor vizate de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate. Inainte de stergere, trebuiesc verificate excepțiile prevăzut de art. 17 alin (3) al GDPR, care permit sau obligă să se păstreze datele, chiar și în ipoteza formulării unei cereri de ștergere.

D**reptul la ștergere nu se aplică dacă prelucrarea este necesară**:

(a) pentru exercitarea dreptului la liberă exprimare și la informare;

(b) pentru respectarea unei obligații legale care prevede prelucrarea în temeiul dreptului Uniunii sau al dreptului intern care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este învestit operatorul;

(c) din motive de interes public în domeniul sănătății publice, în conformitate cu articolul 9 alineatul (2) literele (h) și (i) și cu articolul 9 alineatul (3);

(d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în măsura în care dreptul menționat la alineatul (1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective; sau

(e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Dreptul la rectificarea datelor

Conform Art. 16 GDPR: persoana vizată are dreptul de a obține de la operator, rectificarea sau completarea datelor cu caracter personal modificate sau inexacte care o privesc.

Dreptul la restricționarea datelor

Art. 18 GDPR: dreptul la restricționarea datelor este un drept cu caracter temporar. Ca urmare a unei astfel de solicitări, operatorul "îngheață" datele oprind prelucrarea lor pentru o anumită perioadă de timp. În toate cazurile, la momentul ridicării restricției de prelucrare, Operatorul trebuie să informeze persoana vizată cu privire la faptul ca s-a ridicat restricția.

Dreptul la portabilitatea datelor

Art. 20 GDPR. Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator.

Dreptul la opoziție

Art. 21 GDPR. Persoana vizată are dreptul de a se opune, prelucrării datelor sale personale, atunci când acestea sunt prelucrate în scop de marketing direct. E foarte important ca, atunci când există prelucrări care ar putea da naștere acestui drept pentru persoana vizată, în informare să fie menționată existența acestui drept.

Dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată

Persoana vizata poate solicita intervenția umană în procesul de prelucrare.

Contractele de prestari-servicii incheiate cu persoane fizice, daca va fi cazul, vor fi completate cu urmatoarele elemente:

1. obiectul și durata prelucrării,
2. natura și scopul prelucrării,
3. tipul de date cu caracter personal,
4. categoriile de persoane vizate,
5. obligațiile și drepturile operatorului.
6. Actiunea imputernicitului este numai pe baza instrucțiunilor scrise ale operatorului (cu excepția cazului în care legea solicită să acționeze fără astfel de instrucțiuni).
7. Asigurarea că persoanele care prelucrează datele sunt supuse unei obligații de confidențialitate.
8. Măsurile adecvate pentru a asigura securitatea prelucrarii

Identificarea unui risc de incalcare a securității datelor cu caracter personal (o încălcare a securității care duce, în mod accidental sau ilegal, la: distrugerea, pierderea, modificarea, divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod sau la accesul neautorizat la acestea) presupune notificarea Autoritatii de Supraveghere.

Daca riscul este riidcat, se notifica si persoana vizata.

Notificarea Autorității de Supraveghere va cuprinde:

• identitatea organizației care face notificarea;

• numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;

• descrierea caracterului incidentului ("ce s-a întâmplat concret", adică);

• acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză;

• acolo unde este posibil, categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;

• descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;

• măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Notificarea persoanelor vizate va cuprinde:

• numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;

• descrierea consecințelor probabile ale încălcării securității datelor cu caracter personal;

• măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

Registrul operațiunilor de prelucrare

In formă scrisă (inclusiv electronic).

Registrul operațiunilor de prelucrare contine:

1. numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;

2. scopurile prelucrării;

3. o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;

4. categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;

5. dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la articolul 49 alineatul (1) al doilea paragraf, documentația care dovedește existența unor garanții adecvate;

6. acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;

7. acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1).

Dacă un împuternicit lucrează cu mai mulți operatori, trebuie să realizeze un astfel de registru pentru fiecare operator în numele căruia lucrează.

Masuri imediate ce vor fi intreprinse de ELECTRO GEAD SRL , in aplicarea prezentei proceduri:

- instruirea personalului propriu, pentru responsabilizare si aplicarea corecta a prevederilor Regulamentului 679/2016;
- acord de prelucrare a datelor cu caracter personal ale persoanelor fizice cu calitatea de salariati sau clienti (pot fi sub forma de acte aditionale la CIM, anexe, acorduri individuale, prevederi inserate in facturi sau alte documente comerciale, etc.);
- completarea contractelor de prestari servicii incheiate cu persoane juridice, cu precizari referitoare la prelucrarea datelor cu caracter personal prin prisma realizarii obiectului acestora;
- intocmirea Registrului pentru evidenta operatiunilor de prelucrare a datelor cu caracter personal;

Administrator ,

CIUCU-HABEANU GHEORGHE