Politica de prelucrare a datelor cu caracter personal

ICCO
Brasov, str. Spicului nr. 3

CUPRINS

I. Scopul politicii de protectie a datelor

Ca parte a responsabilitatii sale sociale, ICCO se angajeaza sa respecte legile nationale si internationale privind prelucrarea si protectia datelor personale. Aceasta politica de protectie a datelor se aplica de catre ICCO si se bazeaza pe principiile de baza acceptate la nivel european privind protectia datelor. Asigurarea masurilor tehnice si procedurale a protectiei datelor reprezinta fundamentul relatiilor de afaceri de incredere si reputatia ICCO ca angajator.
Politica de protectie a datelor este una dintre conditiile-cadru necesare desfasurarii activitatii noastre. Acesta asigura nivelul adecvat de protectie a datelor, prevazut conform GDPR, privind protectia datelor si legile nationale privind gestionarea datelor personale.

II. Domeniul de aplicare politicii de protectie a datelor

Aceasta politica de protectie a datelor se aplica tuturor angajatilor, contactorilor si colaboratorilor ICCO, tuturor companiilor imputernicite sau terte, companiilor afiliate si angajatilor acestora. In acest caz, "imputernicite sau terte" inseamna ca ICCO poate impune adoptarea directa sau indirecta a acestei Politici de protectie a datelor, pe baza contractuala, prin acord. Politica privind protectia datelor se extinde la toate prelucrarile de date cu caracter personal. In tarile in care datele persoanelor juridice sunt protejate in aceeasi masura cu datele personale, aceasta politica de protectie a datelor se aplica in mod egal si datelor persoanelor juridice. Datele anonimizate, de ex. pentru evaluari sau studii statistice, nu sunt supuse acestei politici de protectie a datelor.
Politicile suplimentare de protectie a datelor pot fi create in acord cu Responsabilul de protectie a datelor numai daca sunt cerute de legile nationale aplicabile. Aceasta politica de protectie a datelor poate fi modificata in coordonare cu Responsabilul de protectie a datelor in conformitate cu procedura definita pentru modificarea politicilor. Modificarile vor fi comunicate imediat companiilor partenere ale ICCO, utilizand procesul de modificare a politicilor. Modificarile care au un impact major asupra respectarii politicii de protectie a datelor vor fi raportate autoritatilor de protectie a datelor care supravegheaza aceasta politica de protectie a datelor.
Cea mai recenta versiune a politicii de protectie a datelor poate fi accesata impreuna cu informatiile privind confidentialitatea datelor pe site-ul SC ICCO SRL, http://www.icco.ro.

III. Aplicarea legislatiei nationale

Aceasta politica de protectie a datelor cuprinde principiile de confidentialitate acceptate pe plan international, fara a inlocui legile nationale existente. Acesta completeaza legile nationale privind confidentialitatea datelor. Legea romana relevanta va avea prioritate in cazul in care aceasta este in contradictie cu aceasta politica de protectie a datelor sau are cerinte mai stricte decat aceasta politica. Continutul acestei

politici de protectie a datelor va fi, de asemenea, sa fie respectat in absenta legislatiei nationale corespunzatoare. Vor fi respectate cerintele de raportare pentru prelucrarea datelor conform legislatiei nationale.
ICCO este responsabil de respectarea acestei politici de protectie a datelor si a obligatiilor legale. Daca exista motive sa se creada ca obligatiile legale contravin indatoririlor din cadrul acestei Politici de protectie a datelor, trebuie sa fie informat Responsabilul cu Protectia Datelor. In cazul unor conflicte intre legislatia nationala si politica de protectie a datelor, ICCO va colabora pentru a gasi o solutie practica care sa raspunda scopului politicii de protectie a datelor.

IV.Principii de prelucrare a datelor cu caracter personal

1. Corectitudinea si legalitatea
2. Restrictie la un anumit scop
3. Transparenta
4. Reducerea prelucrarilor si economia datelor
5. Precizia si actualizarea datelor
6. Confidentialitatea si securitatea datelor

V. Fiabilitatea procesarii datelor

Colectarea, prelucrarea si utilizarea datelor cu caracter personal este permisa numai in temeiul necesitatii desfasurarii activitatilor companiei. Orice alta prelucrare care excede ariei de activitati a companiei este interzisa.Ce date prelucram?

1. Date despre clienti si parteneri
1.1 Prelucrarea datelor personale in relatiile contractuale
Datele personale ale potentialilor clienti, clienti si parteneri pot fi prelucrate pentru a stabili, executa si rezilia un contract. Aceasta include, de asemenea, servicii de consultanta pentru partener in cadrul contractului, daca acest lucru este legat de scopul contractual. Inainte de incheierea contractului - in timpul fazei de initiere a contractului - datele personale pot fi prelucrate pentru a pregati ofertele sau comenzile de cumparare sau pentru a indeplini alte cerinte din perspectiva care se refera la incheierea contractului. Persoanele vizate pot fi contactate in timpul procesului de pregatire a contractului, utilizand informatiile pe care le-au furnizat deja. Orice restrictii de prelucrare impuse de legislatia europeana sau nationala sa fie respectate.Pentru activitatile de publicitate ne obligam sa respectam urmatoarele cerinte la punctul V.1.2.

1.2 Prelucrarea datelor in scopuri de marketing
Daca o persoana fizica contacteaza ICCO pentru a solicita informatii (de exemplu, cererea de a primi materiale informative despre un serviciu), prelucrarea datelor pentru a raspunde acestei solicitari este permisa in masura in care corespunde sopului solicitarii.
Acordul,(consimtamantul) privind prelucrarea datelor cu caracter personal in cadrul activitatilor de publicitate este obligatoriu. Datele personale pot

fi prelucrate in scopuri publicitare sau in cadrul cercetarii de piata si de opinie, cu conditia ca acest lucru sa fie compatibil cu scopul pentru care au fost colectate datele initiale. Persoana vizata trebuie informata cu privire la utilizarea datelor sale in scopuri publicitare. Daca datele sunt colectate numai in scopuri publicitare, dezvaluirea de catre persoana vizata este voluntara. Persoana vizata este informata ca furnizarea de date in acest scop este voluntara. Atunci cand se comunica cu persoana vizata, este obtinut in prealabil consimtamantul de a procesa datele in scopuri publicitare. Atunci cand acorda consimtamantul, persoana vizata are posibilitatea de a alege intre formele de contact disponibile, cum ar fi posta obisnuita, e-mail si telefon (Consimtamantul, a se vedea V.1.3).
Daca persoana vizata refuza utilizarea datelor sale in scopuri publicitare, acestea nu mai pot fi utilizate in aceste scopuri si vor fi sa fie blocate de la utilizare in aceste scopuri.

1.3 Consimtamantul in cadrul prelucrarilor
Datele cu caracter personal pot fi procesate numai dupa obtinerea consimtamantului persoanei vizate. Inainte de a da consimtamantul, persoana vizata trebuie informata in conformitate cu IV.3. din aceasta politica de protectie a datelor. Declaratia de aprobare trebuie obtinuta in scris sau in format electronic in scopul documentarii si probarii. In anumite circumstante, cum ar fi conversatiile telefonice, consimtamantul poate fi dat verbal. Acordarea consimtamantului trebuie sa fie obligatoriu probata.

1.4 Prelucrarea datelor personale si legislatia nationala
Prelucrarea datelor cu caracter personal pe teritoriul statului Romania se efectueaza in conformitate cu legea 190/2018 si a Regulamentului European 679, ordine si decizii relevante in acest sens.Recunoastem competenta ANSPDC asupra verificarii legalitatii procedurilor proceselor si masurilor apartinand
domeniului de aplicare a protectiei datelor cu caracter personal. Tipul si amploarea procesarii datelor trebuie sa fie necesare pentru activitatea legala de prelucrare a datelor si respecta dispozitiile legale relevante.

1.5 Prelucrarea datelor urmand un interes legitim
Datele personale pot fi procesate, de asemenea, daca sunt necesare pentru un interes legitim al companiilor din ICCO. Interesele legitime sunt in general de natura juridica (de exemplu, colectarea creantelor restante) sau comerciale (de exemplu, evitarea posibilitatii incalcarilor prevederilor contractului). Datele cu caracter personal nu pot fi prelucrate in scopul unui interes legitim daca, in cazuri individuale, exista dovezi conform carora interesele persoanei vizate merita protectie si ca aceasta are prioritate. Inainte de prelucrarea datelor, este necesar sa se determine daca exista interese care trebuie protejate.

1.6 Prelucrarea datelor cu caracter sensibil
Datele cu caracter personal foarte sensibile pot fi procesate numai daca legea impune acest lucru sau persoana vizata a dat consimtamantul expres. Aceste date pot fi, de asemenea, prelucrate daca este obligatorie

pentru afirmarea, exercitarea sau apararea revendicarilor legale referitoare la persoana vizata. Daca exista intentia de procesare a unor date extrem de sensibile, responsabilul cu protectia datelor cu caracter personal este informat in prealabil.

1.7 Deciziile de prelucrare automate

Prelucrarea automata a datelor cu caracter personal care este utilizata pentru evaluarea anumitor aspecte (de exemplu, bonitatea clientului) si nu poate constitui singura baza pentru deciziile care au consecinte juridice negative sau care ar putea afecta in mod semnificativ persoana vizata. Persoana vizata trebuie informata cu privire la faptele si rezultatele deciziilor individuale automatizate si la posibilitatea de a raspunde. Pentru a evita deciziile eronate, un angajat trebuie sa efectueze un test si o verificare a plauzibilitatii.

1.8 Datele utilizatorului pe internet

Daca datele cu caracter personal sunt colectate, prelucrate si utilizate pe site-uri web sau in aplicatii, persoanele vizate sunt informate despre aceasta intr-o declaratie de confidentialitate si, daca este cazul, informatii despre cookie-uri. Declaratia de confidentialitate si orice informatie privind modulele cookie este disponibila de site-ul nostrum web, integrata astfel incat sa fie usor de identificat, direct accesibile si disponibile in mod consecvent pentru persoanele vizate.

Daca sunt create profiluri de utilizare (urmarire) pentru a evalua utilizarea site-urilor web si a aplicatiilor, persoanele vizate sunt intotdeauna informate in mod corespunzator in declaratia de confidentialitate. Urmarirea personala este efectuata numai dupa consimtamantul persoanei vizate. Daca urmarirea utilizeaza un pseudonim, persoana vizata are posibilitatea de a renunta la declaratia de confidentialitate.

2. Datele personale ale angajatilor

2.1 Prelucrarea datelor angajatilor

In relatiile de munca, datele cu caracter personal pot fi prelucrate, daca este necesar, pentru initierea, executarea si incetarea contractului de munca. La initierea unui raport de munca, datele personale ale solicitantilor pot fi procesate cu consimtamant. In cazul in care candidatul este respins, datele acestuia trebuie sterse in conformitate cu perioada de pastrare necesara, cu exceptia cazului in care solicitantul a fost de acord sa ramana la dosar pentru un viitor proces de selectie. De asemenea, este necesar consimtamantul pentru utilizarea datelor pentru procesele de aplicare suplimentare.

In raportul de munca existent, prelucrarea datelor trebuie sa se refere intotdeauna la scopul contractului de munca daca nu se aplica niciuna dintre urmatoarele circumstante pentru prelucrarea datelor autorizate.

Daca in timpul procedurii de solicitare ar trebui sa fie necesara colectarea de informatii despre un solicitant de la o terta parte, trebuie respectate cerintele legilor nationale corespunzatoare. In caz de indoiala, trebuie obtinut un acord de la persoana vizata.

Trebuie sa existe o autorizatie legala pentru prelucrarea datelor cu caracter personal care au legatura cu relatia de munca, dar care nu a facut parte initial din executarea contractului de munca. Acestea pot include cerinte legale, reglementari colective cu reprezentantii angajatilor, consimtamantul angajatului sau interesul legitim al companiei.

2.2 Prelucrarea datelor la solicitarea autoritatilor legale

Prelucrarea datelor personale ale angajatilor este permisa si in cazul in care legislatia nationala solicita, impune sau autorizeaza acest lucru. Tipul si amploarea procesarii datelor trebuie sa fie necesare pentru activitatea legala de prelucrare a datelor si trebuie sa respecte dispozitiile statutare relevante. Daca exista o anumita flexibilitate juridica, trebuie luate in considerare interesele angajatului care merita protejate.

2.3 Prelucrarea colectiva a datelor personale

IIn cazul in care o activitate de prelucrare a datelor depaseste scopul indeplinirii unui contract, aceasta poate fi permisa daca este autorizata printr-o conventie(acord) colectiva. Acordurile colective sunt acorduri de salarizare sau acorduri incheiate intre angajatori si reprezentantii angajatilor, in limita permisa de legislatia in materie de munca. Acordurile trebuie sa acopere scopul specific al activitatii de prelucrare a datelor intentionate si trebuie intocmite in limitele parametrilor legislatiei nationale privind protectia datelor.

2.4 Consimtamantul angajatului

Datele angajatului pot fi prelucrate dupa consimtamantul persoanei in cauza, inainte de angajare. Declaratiile de consimtamant trebuie prezentate in mod voluntar. Acordul involuntar este nul. Declaratia de aprobare trebuie obtinuta in scris sau in format electronic in scopul documentarii. In anumite circumstante, consimtamantul poate fi dat verbal, caz in care trebuie sa fie documentat corespunzator. In cazul furnizarii informate si voluntare de date de catre partea relevanta, se poate lua consimtamantul daca legislatia nationala nu necesita consimtamantul expres. Inainte de a da consimtamantul, persoana vizata trebuie informata in conformitate cu IV.3. din aceasta politica de protectie a datelor.

2.5 Prelucrarea datelor in urmarirea unui interes legal juridic

Datele personale pot fi procesate, de asemenea, daca este necesar sa se impuna un interes legitim al ICCO. Interesele legitime sunt in general de natura juridica (de exemplu, depunerea, aplicarea sau apararea impotriva revendicarilor legale) sau financiare (de exemplu, evaluarea companiilor).
Datele cu caracter personal nu pot fi prelucrate pe baza unui interes legitim daca, in cazuri individuale, exista dovezi ca interesele angajatului merita protectie. Inainte de prelucrarea datelor, trebuie sa se determine daca exista interese care merita protejate.
Masurile de control care necesita prelucrarea datelor angajatului pot fi luate numai daca exista o obligatie legala de a face acest lucru sau daca exista un motiv legitim. Chiar daca exista un motiv legitim, este examinata

si proportionalitatea masurii de control. Interesele justificate ale societatii in ceea ce priveste executarea masurii de control (de exemplu, respectarea dispozitiilor legale si a normelor interne ale societatii) sunt cantarite impotriva oricaror interese care merita protectie pe care angajatul afectat de masura le poate avea in excluderea sa si nu poate fi efectuata decat daca este cazul. Interesul legitim al companiei si orice interese ale angajatului care merita protejat trebuie sa fie identificate si documentate inainte de luarea oricaror masuri. In plus, sunt luate in considerare orice cerinte suplimentare din legislatia nationala (de exemplu, drepturile de co-determinare pentru reprezentantii angajatilor si drepturile de informare ale persoanelor vizate)

2.6 Prelucrarea datelor sensibile

Datele cu caracter personal foarte sensibile pot fi procesate numai in anumite conditii. ICCO nu prelucreaza date despre originea rasiala si etnica, convingerile politice, convingerile religioase sau filozofice, calitatea de membru al sindicatelor si sanatatea si viata sexuala a persoanei vizate. In conformitate cu legislatia nationala, alte categorii de date pot fi considerate extrem de sensibile sau continutul categoriilor de date poate fi completat diferit. Mai mult, datele care se refera la o infractiune pot fi procesate adesea numai in conformitate cu cerintele speciale din legislatia nationala.

Prelucrarea datelor privind starea de sanatate a angajatilor este permisa in scopul indeplinirii unor cerinte legale. Angajatul se obliga de asemenea, sa consimta in mod expres prelucrarea.

Daca exista planuri de procesare a unor date extrem de sensibile, responsabilul cu protectia datelor cu caracter personal trebuie sa fie informat in prealabil.

2.7 Deciziile de prelucrare automata

In cazul in care datele personale sunt prelucrate automat ca parte a relatiei de munca si sunt evaluate datele personale specifice (de exemplu, in cadrul selectiei personalului sau al evaluarii profilurilor de competente), aceasta prelucrare automata nu poate constitui singura baza pentru deciziile care ar avea consecinte negative sau probleme semnificative pentru angajatul afectat. Pentru a evita deciziile eronate, procesul automatizat trebuie sa asigure ca o persoana fizica evalueaza continutul situatiei si ca aceasta evaluare este baza deciziei. Persoana vizata trebuie, de asemenea, sa fie informata cu privire la faptele si rezultatele deciziilor individuale automatizate si la posibilitatea de a raspunde.

2.8 Telecomunicatii si internet/monitorizari prin GPS

Echipamentele telefonice, adresele de e-mail, intranetul si internetul impreuna cu retelele sociale interne sunt furnizate de companie in primul rand pentru activitati legate de munca. Ele sunt un instrument si o resursa a companiei. Acestea pot fi utilizate in cadrul reglementarilor legale aplicabile si al politicilor interne ale companiei. In cazul utilizarii autorizate in scopuri personale, legile privind secretul telecomunicatiilor si legile nationale privind telecomunicatiile trebuie respectate, daca este cazul.

Nu exista o monitorizare generala a comunicatiilor telefonice si de e-mail sau a utilizarii intranetului/internetului, cu exceptia monitorizarii autoturismelor companiei dotate cu sistem autorizat de urmarire prin GPS. Pentru a ne apara impotriva atacurilor asupra infrastructurii IT sau a utilizatorilor individuali, pot fi implementate masuri de protectie pentru conexiunile la reteaua ICCO care blocheaza continutul daunator din punct de vedere tehnic sau care analizeaza modelele de atac. Din motive de securitate, utilizarea echipamentelor telefonice, a adreselor de e-mail, a retelelor intranet / internet si a retelelor sociale interne poate fi inregistrata pentru o perioada temporara. Evaluarile acestor date de la o anumita persoana pot fi facute numai intr-un caz concret si justificat de incalcari suspectate a legilor sau politicilor ICCO. Evaluarile pot fi efectuate numai de catre departamentele de investigaresauautoritatile competente, asigurandu-se, in acelasi timp, respectarea principiului legalitatii si proportionalitatii. Legislatia nationala relevanta trebuie respectata in acelasi mod ca si regulamentul .

VI.Transferul datelor cu caracter personal

Transmiterea datelor cu caracter personal catre destinatarii din afara sau in interiorul ICCO este supusa cerintelor de autorizare pentru prelucrarea datelor cu caracter personal in conformitate cu sectiunea V. Beneficiarul datelor trebuie sa utilizeze datele numai in scopurile definite.
In cazul in care datele sunt transmise unui destinatar din afara tarii sau catre o tara terta, aceasta tara trebuie sa implementeze/accepte sa mentina un nivel de protectie a datelor echivalent cu aceasta politica de protectie a datelor. Este necesar acordul persoanei vizate inainte activitatilor de transfer.In cazul in care datele sunt transmise de o terta parte catre ICCO, trebuie sa se asigure ca datele pot fi utilizate in scopul urmarit.

VII. Prelucrarea datelor personale in cadrul contractelor comerciale

Prelucrarea datelor de catre o persona/societate imputernicita inseamna ca un procesator este angajat sa proceseze date cu caracter personal in numele si pentru ICCO si este obligat a-si asuma responsabilitatea pentru procesul de prelucrare conex. In aceste cazuri, un acord privind prelucrarea datelor cu
privire la procesator (persoana imputernicit) va fi incheiat si va avea la baza un contract in acest sens. Persona imputernicita de noi are intreaga responsabilitate pentru prelucrarea corecta si legala a datelor. Procesatorul poate procesa date personale numai conform instructiunilor noastre. La emiterea ordinului, trebuie indeplinite cerinte minime de securitate; departamentul care plaseaza comanda trebuie sa se asigure ca acestea sunt indeplinite.
Procesatorul(persoana imputernicita) trebuie ales pe baza capacitatii sale de a acoperi masurile de protectie tehnice si organizatorice necesare. Ordinul trebuie trimis in scris. Instructiunile privind prelucrarea datelor si responsabilitatile trebuie sa fie documentate.

Vor fi luate in considerare standardele minimale tehnice si organizatorice pentru protectia datelor furnizate de Responsabil Protectia Datelor.
Inainte de inceperea prelucrarii datelor, vom verifica daca persoana imputernicita isi va respecta obligatiile. Un procesator poate documenta conformitatea cu cerintele de securitate a datelor, in special prin prezentarea unei certificari adecvate. In functie de riscul de prelucrare a datelor, revizuirile vor fi repetate in mod regulat pe durata contractului.
In cazul procesarii transfrontaliere a datelor din contracte, trebuie indeplinite cerintele nationale relevante pentru transmiterea datelor cu caracter personal in strainatate.
In special, datele cu caracter personal din Spatiul Economic European pot fi prelucrate intr-o tara terta numai daca furnizorul poate dovedi ca are un standard de protectie a datelor echivalent cu aceasta politica de protectie a datelor. Instrumentele adecvate pot fi:
Acordul privind clauzele contractuale standard ale UE pentru prelucrarea datelor din contracte in tarile terte cu furnizorul si cu orice subcontractanti.
Participarea procesatorului la un sistem de certificare acreditat de UE pentru asigurarea unui nivel suficient de protectie a datelor.
Recunoasterea regulilor corporative obligatorii ale procesatorului pentru a crea un nivel adecvat de protectie a datelor de catre autoritatile de supraveghere responsabile pentru protectia datelor.

VIII. Drepturile persoanei vizate

Fiecare persoana vizata are urmatoarele drepturi. Acestea vor fi respectate imediat de unitatea noastra si nu poate constitui un dezavantaj pentru persoana vizata.

1. Persoana vizata poate solicita informatii privind datele cu caracter personal care i-au fost stocate, modul in care au fost colectate datele si in ce scop. Daca exista alte drepturi de a vizualiza documentele noastre (de exemplu, dosarul personalului) pentru relatia de munca in conformitate cu legile relevante privind ocuparea fortei de munca, acestea nu vor fi afectate.
2. Daca datele cu caracter personal sunt transmise tertilor, vor fi furnizate informatii despre identitatea destinatarului sau categoriile de destinatari.
3. Daca datele cu caracter personal sunt incorecte sau incomplete, persoana vizata poate solicita corectarea sau completarea acesteia.
4. Persoana vizata poate contesta prelucrarea datelor sale in scopuri de publicitate sau de cercetare a pietei / opiniei publice. Datele trebuie sa fie blocate de aceste tipuri de utilizare.
5. Persoana vizata poate cere ca datele sale sa fie sterse in cazul in care prelucrarea acestor date nu are un temei juridic sau daca temeiul juridic nu mai este valabil. Acelasi lucru este valabil daca scopul din spatele procesarii datelor a expirat sau a incetat sa mai fie aplicabil din alte motive. Perioadele de pastrare existente si interesele conflictuale care merita protejate trebuie respectate.

6. Persoana vizata are, in general, dreptul de a se opune prelucrarii datelor sale si aceasta trebuie luata in considerare daca protectia intereselor sale are prioritate fata de interesele operatorului de date datorita unei situatii personale specifice. Acest lucru nu se aplica in cazul in care o dispozitie legala impune ca datele sa fie procesate.
In plus, fiecare persoana vizata poate pretinde drepturile de la punctul III. Paragraf 2, IV, V, VI, IX, X si XIV. Paragraf 3 ca beneficiar tert daca noi, care am acceptat sa respectam politica de protectie a datelor nu respectam cerintele si incalcam drepturile partii.

IX.Confidentialitatea procesarii

Datele personale sunt supuse secretului confidentialiatii de date. Orice colectare, prelucrare sau utilizare neautorizata a acestor date de catre angajati este interzisa. Orice prelucrare de date efectuata de un angajat pe care nu a fost autorizata sa o indeplineasca ca parte a indatoririlor sale legitime este neautorizata. Se aplica principiul "necesitatii de a cunoaste". Angajatii pot avea acces la informatii personale numai dupa cum este adecvat pentru tipul si scopul sarcinii in cauza. Acest lucru necesita o defalcare si separare atenta, precum si punerea in aplicare a rolurilor si responsabilitatilor.
Angajatilor li se interzice sa utilizeze date cu caracter personal in scopuri private sau comerciale, sa le dezvaluie persoanelor neautorizate sau sa le puna la dispozitie in orice alt mod. Ne vom instrui angajatii la inceputul relatiei de munca cu privire la obligatia de a proteja secretul datelor. Aceasta obligatie ramane in vigoare chiar si dupa incheierea perioadei de angajare.

X. Securizarea datelor

Datele personale sunt protejate impotriva accesului neautorizat si a prelucrarii sau dezvaluirii ilegale, precum si a pierderii, modificarii sau distrugerii accidentale. Acest lucru se aplica indiferent daca datele sunt prelucrate electronic sau pe suport de hartie. Inainte de introducerea noilor metode de prelucrare a datelor, in special a noilor sisteme informatice, trebuie definite si implementate masuri tehnice si organizatorice de protectie a datelor cu caracter personal. Aceste masuri trebuie sa se bazeze pe stadiul tehnicii, pe riscurile procesarii si pe necesitatea de a proteja datele (determinate de procesul de clasificare a informatiilor).
In special, departamentul responsabil se poate consulta cu responsabilul de protectia datelor. Masurile tehnice si organizatorice pentru protejarea datelor cu caracter personal fac parte din managementul securitatii informatiilor si trebuie adaptate in mod continuu la evolutiile tehnice si la schimbarile organizatorice.
Urmatoarele procese si proceduri sunt implementate la nivelul companiei ICCO:
1. Acces: Angajatii care proceseaza date cu carcater personal, pentru a obtine acces la o baza de date cu caracter personal, trebuie sa se identifice.

Identificarea se face prin introducerea codului de identificare de la tastatura (username si parola). Fiecare utilizator are propriul sau cod de identificare. Parola este schimbata la 6 luni. Orice utilizator proceseaza date cu caracter personal are semnat un angajament de confidentialitate. Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se va face pe baza unei liste aprobate de catre Responsabil Protectie Date.

2. Tipul de acces: Utilizatorii nostru acceseaza numai datele cu caracter personal necesare pentru indeplinirea atributiilor lor de serviciu: administrare, introducere, prelucrare, salvare si dupa actiuni aplicate asupra datelor cu caracter personal (cum ar fi: scriere, citire, stergere), precum si procedurile privind aceste tipuri de acces. Programatorii sistemelor de prelucrare a datelor cu caracter personal nu vor avea acces la datele cu caracter personal. ICCO permite accesul programatorilor la datele cu caracter personal dupa ce acestea au fost transformate in date anonime. Compartimentul IT tehnic poate avea acces la datele cu caracter personal pentru rezolvarea unor cazuri exceptionale. Operatorul va stabili modalitatile stricte prin care se vor distruge datele cu caracter personal. Autorizarea pentru aceasta prelucrare de date cu caracter personal trebuie limitata la utilizatori.

3. ICCO a desemnat utilizatori autorizati pentru operatiile de colectare si introducere de date cu caracter personal intr-un sistem informational. Orice modificare a datelor cu caracter personal se poate face numai de catre utilizatori autorizati desemnati de DPO. Sistemul informatic are posibilitatea sa inregistreze cine a facut modificarea, data si ora modificarii.

4. Executia copiilor de siguranta. ICCO a stabilit ca la o perioada de 3 luni se vor executa copiile de siguranta ale bazelor de date cu caracter personal, precum si ale programelor folosite pentru prelucrarile automatizate. Copiile de siguranta se vor stoca in camere cu acces restrictionat, cu masuri de securitate video.

5. Computerele si terminalele de acces Computerele si alte terminale de acces sunt dispuse in incaperi monitorizate video/ sisteme de control acces.

6. Fisierele de acces. Orice accesare a bazei de date cu caracter personal este inregistrata intr-un fisier de acces (numit log la prelucrarile automate). Informatiile inregistrate in fisierul de acces sau in registru vor fi:

- codul de identificare (numele utilizatorului pentru bazele de date cu caracter personal manuale);
- numele fisierului accesat (fisei);
- numarul inregistrarilor efectuate;
- tipul de acces;
- codul operatiei executate sau programul folosit;
- data accesului (an, luna, zi);
- timpul (ora, minutul, secunda).

Pentru prelucrarile automate aceste informatii vor fi stocate intr-un fisier de acces general sau in fisiere separate pentru fiecare utilizator. Pastram fisierele de acces cel putin minim 5 ani. Fisierele de acces au posibilitatea de identificarea de a persoanelor care au accesat date cu caracter personal

fara un motiv anume, in vederea aplicarii unor sanctiuni sau a sesizarii organelor competente.
7. Utilizatorii care au acces la date cu caracter personal sunt instruiti de asupra confidentialitatii acestora si vor fi avertizati prin mesaje care vor aparea pe monitoare in timpul activitatii. Utilizatorii sunt obligati sa isi inchida sesiunea de lucru atunci cand parasesc locul de munca.
8. Pentru mentinerea securitatii prelucrarii datelor cu caracter personal (in special impotriva virusilor informatici) ICCO a implementat urmatoarele masuri:
a)interzicerea folosirii de catre utilizatori a programelor software care provin din surse externe;
b)informarea utilizatorilor in privinta pericolului privind virusii informatici;
c)implementarea unor sisteme automate de devirusare si de securitate a sistemelor informatice;
9. Imprimarea datelor Scoaterea la imprimanta a datelor cu caracter personal se efectueaza numai de utilizatori autorizati pentru aceasta operatiune. Sunt implementate proceduri interne specifice privind folosirea si distrugerea acestor materiale

XI.Controlul prelucrarii datelor cu caracter personal

Respectarea politicii de protectie a datelor si a legilor aplicabile privind protectia datelor este verificata in mod regulat prin intermediul auditurilor de protectie a datelor si al altor controale. Performanta acestor controale este responsabilitatea Responsabilului Protectiei Datelor Personale. Rezultatele controalelor privind protectia datelor trebuie raportate directorului pentru protectia datelor cu caracter personal. La cerere, rezultatele controalelor privind protectia datelor vor fi puse la dispozitia autoritatii responsabile de protectia datelor. Autoritatea responsabila cu protectia datelor poate efectua propriile controale de conformitate cu reglementarile din aceasta politica, asa cum le permite legislatia nationala.

XII. Incidente date cu caracter personal

Toti angajatii trebuie sa informeze imediat Responsabilul cu Protectia Datelor privind cazurile de incalcare a acestei Politici de protectie a datelor sau alte reglementari privind protectia datelor cu caracter personal (incidente de protectie a datelor) in cazurile de:
- Transmiterea necorespunzatoare a datelor cu caracter personal catre terte parti,
- Accesul neadecvat al tertilor la datele cu caracter personal sau
- Pierderea datelor cu caracter personal.
Rapoartele impuse de companie (Gestionarea incidentelor de securitate a informatiilor) trebuie facute imediat, astfel incat sa poata fi respectate toate obligatiile de raportare in conformitate cu legislatia nationala.

XIII. Raspunderi si sanctiuni

Directorii ICCO si departamentele executive ale societatiii sunt responsabile de prelucrarea datelor in zona lor de responsabilitate. Prin urmare, acestia sunt obligati sa se asigure ca sunt indeplinite cerintele legale si cele continute in politica de protectie a datelor pentru protectia datelor (de exemplu, obligatiile nationale de notificare). Personalul de conducere are responsabilitatea de a se asigura ca exista masuri organizationale, resurse umane si tehnice pentru ca orice prelucrare
a datelor sa fie efectuata in conformitate cu protectia datelor. Respectarea acestor cerinte este responsabilitatea angajatilor relevanti. Daca agentiile oficiale efectueaza controale de protectie a datelor, responsabilul cu Protectia datelor trebuie informat imediat.
Din punct de vedere organizational, Responsabilul pentru protectia datelor reprezinta consilierul ICCO pentru operatiunile de protectie a datelor cu caracter personal. Departamentele responsabile cu procesele si proiectele de afaceri trebuie sa informeze a datelor in timp util cu privire la noua prelucrare a datelor cu caracter personal. Pentru planurile de prelucrare a datelor care pot prezenta riscuri speciale pentru drepturile individuale ale persoanelor vizate, Responsabilul Protectia Datelor va fi informat inainte de inceperea procesarii. Acest lucru se aplica in special datelor cu caracter personal extrem de sensibile. Managerii trebuie sa se asigure ca angajatii lor sunt suficient de instruiti in protectia datelor.
Prelucrarea necorespunzatoare a datelor cu caracter personal sau alte incalcari ale legilor privind protectia datelor pot fi urmarite penal in numeroase tari si duc la cereri de despagubire pentru daune. Incalcarile pentru care angajatii individuali sunt responsabili pot conduce la sanctiuni conform legii muncii.

Responsabil Protectia Datelor