POLITICA COMPANIEI

privind aplicarea REGULAMENTULUI (UE) 2016/679 al PARLAMENTULUI EUROPEAN si al CONSILIULUI din 27 aprilie 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE

REGULAMENTUL GENERAL PRIVIND PROTECTIA DATELOR (GDPR)

CUPRINS

PARTEA I – ASPECTE GENERALE

Societatea **H&S WEST PROPERTIES SRL**, cu sediul social in Bucuresti, sector 1, Calea Victoriei, nr. 109, tronson 1, parter, biroul nr. 68, Romania, inregistrata la Oficiul Registrului Comertului sub nr. J40/15295/2015, cod fiscal RO 35332797, email office@mc-group.ro, tel. 0744 130 471, reprezentata de administratori Dl. Ziv-Asher Tetelman si Dl. Shahar Machat,
Societatea **HAGAG DEVELOPMENT VICTORIEI 139 S.R.L.,** cu sediul social in Bucuresti, sector 1, Calea Victoriei, nr. 109, parter, biroul nr. 60, Romania, înregistrată la Registrul Comerţului sub nr. J40/16012/2017, Cod Unic de Înregistrare 38232008, email office@mc-group.ro, tel. 0744 130 471, reprezentata de administrator Dl. Shahar Machat,
Societatea **H VICTORIA STIRBEI GALLERIES S.R.L.,** cu sediul social in Bucuresti, sector 1, Calea Victoriei, nr. 109, parter, biroul nr. 66, Romania, înregistrată la Registrul Comerţului sub nr. J40/988/2017, Cod Unic de Înregistrare 36984373, email office@mc-group.ro, tel. 0744 130 471, reprezentata de administrator Dl. Shahar Machat,
Societatea **H PIPERA FOREST S.R.L.**, cu sediul social in Calea Victoriei nr. 109, parter, biroul nr. 57, sector 1, Bucuresti, înregistrată la Oficiul Registrului Comerţului sub nr. J40/7281/2017, cod fiscal 37604367, email office@mc-group.ro, tel. 0744 130 471, reprezentată de administrator Dl. Shahar Machat,
Societatea **HAGAG DEVELOPMENT PALLADY 66 S.R.L.,** cu sediul social in Bucuresti, sector 1, Calea Victoriei, nr. 109, parter, biroul nr. 69, Romania, înregistrată la Registrul Comerţului sub nr. J40/20145/2006, Cod Unic de Înregistrare RO 19419078, email office@mc-group.ro, tel. 0744 130 471, reprezentata de administratori Dl. Tetelman Ziv-Asher si Dl. Shahar Machat,
Societatea **H&S EAST PROPERTIES S.R.L.,** cu sediul social in Bucuresti, sector 1, Calea Victoriei, nr. 109, parter, biroul nr. 58, Romania, înregistrată la Registrul Comerţului sub nr. J40/15893/2017, Cod Unic de Înregistrare 38224269, email office@mc-group.ro, tel. 0744 130 471, reprezentata de administrator Dl. Tetelman Ziv-Asher,
Societatea **H&S SOUTH PROPERTIES S.R.L.,** cu sediul social in Bucuresti, sector 1, Calea Victoriei, nr. 109, parter, biroul nr. 64, Romania, înregistrată la Registrul Comerţului sub nr. J40/15870/2017, Cod Unic de Înregistrare 38223573, email office@mc-group.ro, tel. 0744 130 471, reprezentata de administrator Dl. Tetelman Ziv-Asher,
Societatea **H GROUP PROPERTIES INVEST S.R.L.,** cu sediul social in Bucuresti, sector 1, Calea Victoriei, nr. 109, parter, biroul nr. 65, Romania, înregistrată la Registrul Comerţului sub nr. J40/15892/2017, Cod Unic de Înregistrare 38224242, email office@mc-group.ro, tel. 0744 130 471, reprezentata de administrator Dl. Tetelman Ziv-Asher,

denumite in cele ce urmeaza “compania” si/sau “societatea”,

se aliniaza prevederilor Regulamentului general privind protectia datelor (denumit in cele ce urmeaza “GDPR”) prin urmatoarele:

Prezenta procedura stabileste masuri tehnice (scriptice si fizice) si organizatorice pentru prelucrarea datelor cu caracter personal, precum si pentru normele referitoare la libera circulatie a datelor cu caracter personal si are ca scop stabilirea unor norme de conduita pentru asigurarea unui nivel satisfacator de protectie a datelor cu caracter personal prelucrate de catre societate si informarea specifica si lipsita de ambiguitate a persoanelor vizate cu privire la scopurile prelucrarii, temeiul juridic al prelucrarii, durata prelucrarii, destinatarii datelor cu caracter personal colectate si modalitatile de exercitare a drepturilor individuale.

In cadrul operatiunii de prelucrare a datelor, societatea tine seama de reglementarile legale in vigoare in aceasta materie, respecta si aplica principiile care stau la baza protectiei datelor personale si asigura confidentialitatea si securitatea datelor prin masuri organizatorice si tehnice adecvate, concretizate in proceduri interne, reguli de conduita si training-uri continue de constientizare si responsabilizare a angajatilor sai.
Colectarea de date cu caracter personal prin mijloace frauduloase, neloiale sau ilegale este interzisa. Persoanele vizate vor fi informate asupra categoriilor de date care sunt prelucrate, scopul prelucrarii, precum si consecintele refuzului acestora de a furniza companiei datele solicitate. Scopurile pentru care se colecteaza date se precizeaza in scris, intr-un limbaj usor accesibil pentru persoanele vizate.

Scopul principal pentru care societatea colecteaza date cu caracter personal il reprezinta incheierea si executarea diferitelor contracte, precum si a tuturor actelor/documentelor/notificarilor/informarilor in legatura cu acestea.

Informatiile inregistrate sunt destinate utilizarii de catre societate si pot fi transmise si/sau accesate, nelimitativ, urmatoarelor categorii de destinari: angajati ai societatii, antreprenor general, parteneri contractuali, alte companii din acelasi grup, autoritate judecatoreasca, birouri notariale, autoritati publice centrale, societati bancare.

Societatea colecteaza urmatoarele date personale:
• numele si prenumele;
• varsta;
• locul si data nasterii;
• codul numeric personal (CNP) sau echivalentul acestuia;
• numarul si seria documentului de identitate;
• data eliberarii documentului de identitate si entitatea care l-a emis;
• domiciliul stabil/resedinta (adresa completa - strada, numar, bloc, scara, etaj, apartament, oras, judet/sector, cod postal, tara);
• nationalitatea/cetatenia;
• telefonul/faxul/ e-mail;
• ocupatia/functia/statutul social (dupa caz);
• datele din actele de stare civila/permis de conducere/certificat de inmatriculare/carte de identitate vehicul (dupa caz);
• date despre persoane aflate in intretinere sau membri ai familiei;

• imagine;
• informatii bancare;
• adresa IP, atunci cand vizitati pagina noastra de internet fara a dezactiva Cookies;
• semnatura.

I. GLOSAR

„GDPR", „Regulamentul" - Regulamentul (UE) 2016/679 al Parlamentului European si al Consiliului din 27 aprilie 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE (Regulamentul general privind protectia datelor, in limba engleza *General Data Protection Regulation*);

„date cu caracter personal" - orice informatii privind o persoana fizica identificata sau identificabila („persoana vizata"); o persoana fizica identificabila este o persoana care poate fi identificata, direct sau indirect, in special prin referire la un element de identificare, cum ar fi un nume, un numar de identificare, date de localizare, un identificator online sau la unul sau mai multe elemente specifice, proprii identitatii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

"prelucrare" - inseamna orice operatiune sau set de operatiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fara utilizarea de mijloace automatizate, cum ar fi colectarea, inregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispozitie in orice alt mod, alinierea sau combinarea, restrictionarea, stergerea sau distrugerea;

„operator" - inseamna persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care, singur sau impreuna cu altele, stabileste scopurile si mijloacele de prelucrare a datelor cu caracter personal; atunci cand scopurile si mijloacele prelucrarii sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevazute in dreptul Uniunii sau in dreptul intern;

„persoana imputernicita de operator" - inseamna persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care prelucreaza datele cu caracter personal in numele operatorului;

„destinatar" - inseamna persoana fizica sau juridica, autoritatea publica, agentia sau alt organism careia (caruia) ii sunt divulgate datele cu caracter personal, indiferent daca este sau nu o parte terta. Cu toate acestea, autoritatile publice carora li se pot comunica date cu caracter personal in cadrul unei anumite anchete in conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de catre autoritatile publice respective respecta normele aplicabile in materie de protectie a datelor, in conformitate cu scopurile prelucrarii;

„parte terta" - inseamna o persoana fizica sau juridica, autoritate publica, agentie sau organism altul decat persoana vizat a, operatorul, persoana imputernicita de operator si persoanele care, sub directa autoritate a operatorului sau a persoanei imputernicite de

operator, sunt autorizate sa prelucreze date cu caracter personal;

„consimtamant” - al persoanei vizate inseamna orice manifestare de vointa libera, specifica, informata si lipsita de ambiguitate a persoanei vizate prin care aceasta accepta, printr-o declaratie sau printr-o actiune fara echivoc, ca datele cu caracter personal care o privesc sa fie prelucrate;

„incalcarea securitatii datelor cu caracter personal” - inseamna o incalcare a securitatii care duce, in mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizata a datelor cu caracter personal transmise, stocate sau prelucrate intr-un alt mod, sau la accesul neautorizat la acestea;

„reprezentant” - inseamna o persoana fizica sau juridica stabilita in Uniune, desemnata in scris de catre operator sau persoana imputernicita de operator in temeiul articolului 27 din GDPR, care reprezinta operatorul sau persoana imputernicita in ceea ce priveste obligatiile lor respective care le revin in temeiul GDPR;

„reguli corporatiste obligatorii” - inseamna politicile in materie de protectie a datelor cu caracter personal care trebuie respectate de un operator sau de o persoana imputernicita de operator stabilita pe teritoriul unui stat membru, in ceea ce priveste transferurile sau seturile de transferuri de date cu caracter personal catre un operator sau o persoana imputernicita de operator in una sau mai multe tari terte in cadrul unui grup de intreprinderi sau al unui grup de intreprinderi implicate intr-o activitate economica comuna;

„autoritate de supraveghere” - inseamna o autoritate publica independenta instituita de un stat membru in temeiul articolului 51 GDPR;

DPO - responsabilul cu protectia datelor (in limba engleza, *data protection officer*);

A29 GL, WP29 - Grupul de Lucru Art. 29 (in limba engleza, Article 29 Working Party), organism consultativ independent al Uniunii Europene in domeniul protectiei si securitatii datelor, format din reprezentanţii autorităţilor de supraveghere a prelucrarii datelor personale din statele membre ale Uniunii Europene;

DPIA - Evaluarea impactului asupra protectiei datelor (in limba engleza, *data-protection impact assessment, DPIA*);

II. PRIVIRE GENERALA ASUPRA NOULUI CADRU LEGAL IN MATERIA PROTECTIEI DATELOR CU CARACTER PERSONAL

A. SFERA DE CUPRINDERE

Prezenta procedura a fost adoptata de societate si are drept scop explicitarea principalelor prevederi ale GDPR pentru a facilita aplicarea acestuia si alinierea societatii cu GDPR.

Procedura urmareste doua scopuri fundamentale:

a) Sa constituie un instrument de clarificare si interpretare a prevederilor Regulamentului;
b) Sa puna in aplicare o serie de bune practice, masuri tehnice si organizatorice menite sa asigure aplicarea adecvata si unitara a normelor care guverneaza prelucrarea datelor cu caracter personal.

B. REGULAMENTUL SI IMPACTUL SAU

Incepand cu 25 mai 2018, Regulamentul abroga si inlocuieste Directiva nr. 95/46/EC privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si libera circulatie a acestor date (art. 94 din GDPR).

Regulamentul are aplicabilitate directa in toate Statele Membre in baza Tratatului pentru Functionarea Uniunii Europene. In consecinta, incepand cu 25 mai 2018, Regulamentul inlocuieste si actul normativ-cadru de reglementare interna a acestui domeniu special, Legea nr. 677/2001 pentru protectia persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulatie a acestor date.

Prelucrarea datelor cu caracter personal se va realiza cu respectarea principiilor prevazute in art. 5 din GDPR, respectiv:

a) datele cu caracter personal trebuie prelucrate in mod legal, echitabil si transparent;

b) datele cu caracter personal trebuie prelucrate pentru scopuri determinate, explicite si legitime;

c) datele cu caracter personal trebuie sa fie adecvate, relevante si neexcesive;

d) datele cu caracter personal trebuie sa fie exacte si actualizate;

e) datele cu caracter personal trebuie sa fie pastrate pentru o perioada care nu depaseste perioada necesara prelucrarii pentru scopul identificat;

f) datele cu caracter personal trebuie sa fie prelucrate intr-un mod care asigura securitatea adecvata a acestora.

III. DIFERENTA DINTRE “OPERATOR” SI “PERSOANA IMPUTERNICITA”

Regulamentul consacra regimuri juridice distincte pentru *operator* si *persoana imputernicita*, caracterizate, in esenta, prin faptul ca:

a) Obligatiile *operatorului* sunt mai numeroase decat cele ale *persoanei imputernicite*. De exemplu, cu exceptia unor situatii limitate, operatorul este obligat sa informeze persoanele vizate cu privire la prelucrare si caracteristicile acesteia.

b) Raspunderea *operatorului* este mai extinsa decat cea a *persoanei vizate*, in special din perspectiva cazurilor de raspundere.

c) Drepturile persoanelor vizate se exercita, in principal, in relatia cu *operatorul*, *persoana imputernicita* avand, de principiu, un rol de asistare a *operatorului* in exercitarea acestor drepturi.

Raportat la cele de mai sus, este esen tial sa se stabileasca calificarea drept operator sau persoana imputernicita.

Conform art. 4 din GDPR:

a) *operatorul* este persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care, singur sau impreuna cu altele, stabileste scopurile si mijloacele de prelucrare a datelor cu caracter personal;

b) *persoana imputernicita* de operator este persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care prelucreaza datele cu caracter personal pe seama operatorului.

In calificarea ca *operator*, un rol esential il va avea gradul de control in ceea ce priveste respectiva prelucrare, mai concret:

a) Stabileste compania care vor fi persoanele vizate de prelucrare? (”*Cine?*”)

b) Stabileste compania ce categorii de date vor fi prelucrate? (”*Ce?*”)

c) Stabileste compania pentru ce scop se va realiza prelucrarea? (”*Pentru ce?*”)

d) Stabileste compania cum se va realiza prelucrarea? (”*Cum?*”) – de exemplu, cui se dezvaluie datele cu caracter personal, pentru cat timp se retin datele cu caracter personal etc.

PARTEA A II-A – REGULI DE BUNA PRACTICA PENTRU CONFORMAREA CU GDPR

I. TEMEIURI LEGALE PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL

A. ASPECTE GENERALE

Prelucrarea datelor cu caracter personal se poate realiza in mod legal numai daca se bazeaza pe unul dintre temeiurile juridice prevazute la art. 6 alin. (1) din GDPR, respectiv:

a) Consimtamantul persoanei vizate;

b) Prelucrare necesara pentru incheierea sau executarea unui contract;

c) Prelucrare necesara pentru indeplinirea unei obligatii legale;

d) Prelucrare necesara pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

e) Prelucrare necesara pentru indeplinirea unei sarcini care serveste unui interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul;

f) Prelucrare necesara in scopul intereselor legitime urmarite de operator sau de o parte terta, cu exceptia cazului in care prevaleaza interesele sau drepturile si libertatile fundamentale ale persoanei vizate.

In ceea ce priveste selectarea temeiului juridic de prelucrare adecvat fiecarei categorii de prelucrare de date cu caracter personal, se impun cateva precizari:

a) Tinand cont de scopurile urmarite prin prelucrarea datelor cu caracter personal, primul pas in evaluarea conformitatii unei prelucrari de date este determinarea temeiului juridic in baza caruia se face prelucrarea. Fara un temei juridic corect identificat, prelucrarea este ilegala;

b) Alegerea temeiului de prelucrare trebuie facuta corect de la inceput, schimbarea ulterioara a temeiului, fara justificare adecvata, este echivalenta cu o neconformitate;

c) Alegerea temeiului de prelucrare trebuie documentat (cel mai frecvent, prin evidenta activitatilor de prelucrare);

d) Persoanele vizate trebuie informate cu privire la temeiul prelucrarii, ca principiu, inainte de inceperea prelucrarii.

B. TEMEIURI JURIDICE DE PRELUCRARE IN DETALIU

B.1. Prelucrare pe baza de consimtamant - Art. 6 alin. (1) lit. (a) GDPR

In lumina noilor prevederi ale GDPR, prelucrarea datelor pe baza de consimtamant presupune respectarea unor standarde legale specifice. A prelucra date pe baza consimtamantului inseamna a oferi persoanei vizate libertate de alegere reala si control sporit asupra prelucrarii. Cateva dintre cele mai importante reguli de obtinere si gestionare a consimtamantului sunt:

a) Consimtamant explicit

Consimtamantul trebuie sa fie exprimat in mod explicit, intr-o maniera clara si specifica (manifestare pozitiva a consimtamantului). Utilizarea unor metode de exprimare implicita / tacita a consimtamantului (e.g. casute de acord pre-bifate) nu este o practica legala.

b) Consimtamant nelegat

Furnizarea unui serviciu solicitat de/oferit persoanei vizate nu poate fi conditionata de acordarea consimtamantului pentru prelucrare din partea respectivei persoane, intrucat astfel, consimtamantul nu ar fi liber exprimat.

c) Consimtamant separat

Consimtamantul trebuie solicitat:

(i) in mod separat de termeni si conditii ori de alte documente de informare si prezentare; (ii) in mod specific pentru fiecare scop pentru care se face prelucrare pe acest temei juridic.

d) Consimtamant documentat

Consimtamantul trebuie documentat si dovada acestuia trebuie pastrata. Ca principiu, operatorul trebuie sa poata demonstra cine a dat consimtamantul, cand, prin ce metoda si ce informatii au fost furnizate cu ocazia preluarii consimtamantului.

e) Consimtamant revocabil

Persoana vizata are dreptul de a retrage consimtamantul in orice moment (forma de manifestare a „*dreptului de a fi uitat*"), iar operatorul trebuie sa ofere un mecanism de retragere facil si sa actioneze pentru a da eficienta retragerii in cel mai scurt timp posibil.

Consimtamantul de colectare a datelor cu caracter personal se exprima in scris de persoanele vizate prin completarea si semnarea de note de informare in legatura cu prelucrarea datelor cu caracter personal.

Consimtamantul nu este necesar in urmatoarele cazuri:

- cand prelucrarea este necesara in vederea executarii unui contract sau antecontract la care persoana vizata este parte ori in vederea luarii unor masuri, la cererea acesteia, inaintea incheierii unui contract sau antecontract;

- cand prelucrarea este necesara in vederea protejarii vietii, integritatii fizice sau sanatatii persoanei vizate ori a unei alte persoane amenințate;

- cand prelucrarea este necesara in vederea indeplinirii unei obligatii legale a operatorului;

- cand prelucrarea este necesara in vederea aducerii la indeplinire a unor masuri de interes public sau care vizeaza exercitarea prerogativelor de autoritate publica cu care este investit operatorul sau tertul caruia ii sunt dezvaluite datele;

- cand prelucrarea este necesara in vederea realizarii unui interes legitim al operatorului sau tertului caruia ii sunt dezvaluite datele cu conditia ca acest interes sa nu prejudicieze

interesul sau drepturile si libertatile fundamentale ale persoanei vizate;

- cand prelucrarea priveste datele obtinute din documente accesibile publicului, conform legii;

- cand prelucrarea este facuta exclusiv in scopuri statistice, de cercetare istorica sau stiintifica, iar datele raman anonime pe toata durata prelucrarii.

B.2. Prelucrare necesara pentru incheierea si executarea unui contract - Art. 6 alin. (1) lit. (b) GDPR

Aceasta presupune necesitatea incheierii sau executarii unui contract. Astfel, prelucrarea este legala daca:

a) Exista un contract valabil, pentru a carui executare este necesara prelucrarea de date cu caracter personal;

b) In faza pre-contractuala, la solicitarea persoanei vizate, este nevoie de prelucrarea anumitor date cu caracter personal in vederea incheierii contractului.

In mod contrar, prelucrarea nu se poate baza pe temeiul incheierii / executarii contractului daca:

a) Trebuie prelucrate datele unei persoane, alta decat cea cu care se incheie contractul;

b) Initiativa incheierii contractului apartine operatorului sau unei terte persoane.

B.3. Prelucrare necesara pentru indeplinirea unei obligatii legale - Art. 6 alin. (1) lit. (c) GDPR

Prelucrarea datelor cu caracter personal pe temeiul necesitatii conformarii unei obligatii legale presupune existenta unei norme legale imperative aplicabile operatorului.

Prelucrarea impusa printr-o decizie administrativa / hotarare judecatoreasca poate fi justificata tot prin necesitatea conformarii unei obligatii legale.

Prelucrarea trebuie sa fie necesara conformarii obligatiei legale. Nu poate fi utilizat acest temei daca se poate asigura in mod rezonabil conformarea cu norma legala fara respectiva prelucrare sau printr-o prelucrarea mai putin invaziva.

B.4. Prelucrare necesara pentru indeplinirea unei sarcini care serveste unui interes public - Art. 6 alin. (1) lit. (e) GDPR

Lit. e) a alin. (1) al Art. 6 din GDPR prevede ca prelucrarea se poate realiza in mod legal daca *„e) [...] este necesara pentru indeplinirea unei sarcini care serveste unui interes*

public [...];".

B.5. Prelucrare necesara in scopul unui interes legitim - Art. 6 alin. (1) lit. (f) GDPR

Interesul legitim este cel mai flexibil temei juridic de prelucrare a datelor cu caracter personal si, de aceea, utilizarea sa trebuie calibrata in mod adecvat. Acesta poate fi folosit doar in cazurile in care prelucrarea are un impact minimal asupra persoanelor vizate. Pentru intemeierea pe interesul legitim, prelucrarea datelor cu caracter personal trebuie sa indeplineasca trei tipuri de caracteristici:

a) Scopul legitim

Operatorul trebuie sa urmareasca un interes legitim, al sau sau al unui tert. Interesul legitim poate fi un interes comercial, profesional sau un scop mai larg, de exemplu un interes social.

b) Necesitatea

Prelucrarea trebuie sa fie proportionala si limitata pentru atingerea interesului legitim urmarit. Nu poate fi utilizat acest temei daca respectivul interes poate fi atins printr-o prelucrare mai putin cuprinzatoare.

c) Raportarea la interesele persoanei vizate

Ca principiu, prelucrarea trebuie sa fie previzibila pentru persoana vizata si sa nu creeze un prejudiciu nenecesar persoanei vizate. Nu intotdeauna interesele persoanei vizate trebuie aliniate cu cele ale operatorului. Pot exista situatii in care interesele operatorului pot prevala asupra celor ale persoanei vizate in cadrul unei prelucrari legitime.

C. PRELUCRAREA DE CATEGORII SPECIALE DE DATE SAU REFERITOARE LA CONDAMNARI PENALE SI INFRACTIUNI

C.1. Categorii speciale de date

GDPR defineste categoriile speciale de date astfel: originea rasiala sau etnica, opiniile politice, confesiunea religioasa, convingerile filozofice, apartenenta la sindicate, date genetice, date biometrice pentru identificarea unica a unei persoane fizice, date privind sanatatea sau date privind viata sexuala sau orientarea sexuala ale unei persoane fizice.

Aceste categorii de date sunt considerate sensibile si se impune un standard de protectie superior. Concret, pentru prelucrarea adecvata a acestor categorii de date, pe langa identificarea unui temei de prelucrare potrivit art. 6 din GDPR, se impune indeplinirea si uneia dintre conditiile reglementate de art. 9 alin. (2) din GDPR:

"a) persoana vizata si-a dat consimtamantul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu exceptia cazului in care dreptul Uniunii sau dreptul intern prevede ca interdictia prevazuta la alineatul (1) sa nu poata fi ridicata prin consimtamantul persoanei vizate;

b) prelucrarea este necesara in scopul indeplinirii obligatiilor si al exercitarii unor drepturi specifice ale operatorului sau ale persoanei vizate in domeniul ocuparii fortei de munca si al securitatii sociale si protectiei sociale, in masura in care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de munca incheiat in temeiul dreptului intern care prevede garantii adecvate pentru drepturile fundamentale si interesele persoanei vizate;

c) prelucrarea este necesara pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci cand persoana vizata se afla in incapacitate fizica sau juridica de a-si da consimtamantul;

d) prelucrarea este efectuata in cadrul activitatilor lor legitime si cu garantii adecvate de catre o fundatie, o asociatie sau orice alt organism fara scop lucrativ si cu specific politic, filozofic, religios sau sindical, cu conditia ca prelucrarea sa se refere numai la membrii sau la fostii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente in legatura cu scopurile sale si ca datele cu caracter personal sa nu fie comunicate tertilor fara consimtamantul persoanelor vizate;

e) prelucrarea se refera la date cu caracter personal care sunt facute publice in mod manifest de catre persoana vizata;

f) prelucrarea este necesara pentru constatarea, exercitarea sau apararea unui drept in instanta sau ori de cate ori instantele actioneaza in exercitiul functiei lor judiciare;

g) prelucrarea este necesara din motive de interes public major, in baza dreptului Uniunii sau a dreptului intern, care este proportional cu obiectivul urmarit, respecta esenta dreptului la protectia datelor si prevede masuri corespunzatoare si specifice pentru protejarea drepturilor fundamentale si a intereselor persoanei vizate;

h) prelucrarea este necesara in scopuri legate de medicina preventiva sau a muncii, de evaluarea capacitatii de munca a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistenta medicala sau sociala sau a unui tratament medical sau de gestionarea sistemelor si serviciilor de sanatate sau de asistenta sociala, in temeiul dreptului Uniunii sau al dreptului intern sau in temeiul unui contract incheiat cu un cadru medical si sub rezerva respectarii conditiilor si garantiilor prevazute la alineatul (3);

i) prelucrarea este necesara din motive de interes public in domeniul sanatatii publice, cum ar fi protectia impotriva amenintarilor transfrontaliere grave la adresa sanatatii sau asigurarea de standarde ridicate de calitate si siguranta a asistentei medicale si a medicamentelor sau a dispozitivelor medicale, in temeiul dreptului Uniunii sau al dreptului intern, care prevede masuri adecvate si specifice pentru protejarea drepturilor si libertatilor persoanei vizate, in special a secretului profesional; sau

j) prelucrarea este necesara in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice, in conformitate cu articolul 89 alineatul (1), in baza dreptului Uniunii sau a dreptului intern, care este proportional cu obiectivul urmarit, respecta esenta dreptului la protectia datelor si prevede masuri

corespunzatoare si specifice pentru protejarea drepturilor fundamentale si a intereselor persoanei vizate.”.

C.2. Date referitoare la condamnari speciale si infractiuni

Similar prelucrarii categoriilor speciale de date, prelucrarea datelor referitoare la condamnari penale si infractiuni presupune:

(i) un temei juridic de prelucrare potrivit Art. 6 din GDPR;
(ii) competenta legala (proprie autoritatilor publice) sau o autorizare legala.

GDPR – temeiuri legale pentru prelucrarea datelor cu caracter personal

Consimtamantul	Preambul (32), (42), (43); Art. 6 alin (1) lit. (a): Prelucrarea este permisa daca persoana vizata si-a dat consimtamantul pentru prelucrare.
Incheierea sau executarea unui contract	Preambul (44); Art. 6 alin. (1) lit. (b): Prelucrarea este necesara pentru executarea unui contract la care persoana vizata este parte sau pentru a face demersuri la cererea persoanei vizate inainte de incheierea unui contract.
Indeplinirea unei obligatii legale	Preambul (45); Art. 6 (1) lit. (c); Art. 6 alin. (3): Prelucrarea este necesara in vederea indeplinirii unei obligatii legale care ii revine operatorului.
Interesele vitale	Preambul (46); Art. 6 (1) lit. (d): Prelucrarea este necesara pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice.
Interesul public	Preambul 46; Art. 6 (1) lit. (e): Prelucrarea este necesara pentru indeplinirea unei sarcini care serveste unui interes public sau care rezulta din exercitarea autoritatii publice cu care este investit operatorul.
Interesul legitim	Preambul (47), (48); Art. 6 (1) lit. (f): Prelucrarea este necesara in scopul intereselor legitime urmarite de operator sau de o parte terta, cu exceptia cazului in care prevaleaza interesele sau drepturile si libertatile fundamentale ale persoanei vizate, care necesita protejarea datelor cu caracter personal, in special atunci cand persoana vizata este un copil.
Prelucrarea de date cu caracter personal referitoare la condamnari penale si infractiuni	Art.10: Prelucrarea de date cu caracter personal referitoare la condamnari penale si infractiuni sau la masuri de securitate conexe in temeiul art. 6 alin. (1) se efectueaza numai sub controlul unei autoritati de stat sau atunci cand prelucrarea este autorizata de dreptul Uniunii sau de dreptul intern care prevede garantii adecvate pentru drepturile si libertătile persoanelor vizate. Orice registru cuprinzator al condamnarilor penale se tine numai sub

	controlul unei autoritati de stat.
Prelucrarea de categorii speciale de date cu caracter personal	Preambul (51)-(56); Art. 9: · persoana vizata si-a dat consimtamantul explicit; · prelucrarea este necesara in scopul indeplinirii obligatiilor si al exercitarii unor drepturi specifice ale operatorului sau ale persoanei vizate in domeniul ocuparii fortei de munca si al securitatii sociale si protectiei sociale; · prelucrarea este necesara pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci cand persoana vizata se afla in incapacitate fizica sau juridica de a-si da consimtamantul; · prelucrarea este efectuata in cadrul activitatilor lor legitime si cu garantii adecvate de catre o fundatie, o asociatie sau orice alt organism fara scop lucrativ si cu specific politic, filozofic, religios sau sindical, cu conditia ca prelucrarea sa se refere numai la membrii sau la fostii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente in legatura cu scopurile sale si ca datele cu caracter personal sa nu fie comunicate tertilor fara consimtamantul persoanelor vizate; · prelucrarea se refera la date cu caracter personal care sunt facute publice in mod manifest de catre persoana vizata; · prelucrarea este necesara pentru constatarea, exercitarea sau apararea unui drept in instanta sau ori de cate ori instantele actioneaza in exercitiul functiei lor judiciare; · prelucrarea este necesara din motive de interes public major, in baza dreptului Uniunii sau a dreptului intern, care este proportional cu obiectivul urmarit, respecta esenta dreptului la protectia datelor si prevede masuri corespunzatoare si specifice pentru protejarea drepturilor fundamentale si a intereselor persoanei vizate; · prelucrarea este necesara in scopuri legate de medicina preventiva sau a muncii, de evaluarea capacitatii de munca a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistenta medicala sau sociala sau a unui tratament medical sau de gestionarea sistemelor si serviciilor de sanatate sau de asistenta sociala, in temeiul dreptului Uniunii sau al dreptului intern sau in temeiul unui contract incheiat cu un cadru medical si sub rezerva respectarii conditiilor si garantiilor prevazute la alin. (3); · prelucrarea este necesara din motive de interes public in domeniul sanatatii publice, cum ar fi protectia impotriva amenintarilor transfrontaliere grave la adresa sanatatii

	sau asigurarea de standarde ridicate de calitate si siguranta a asistentei medicale si a medicamentelor sau a dispozitivelor medicale, in temeiul dreptului Uniunii sau al dreptului intern, care prevede masuri adecvate si specifice pentru protejarea drepturilor si libertatilor persoanei vizate, in special a secretului profesional; · prelucrarea este necesara in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice, in conformitate cu art. 89 alin. (1), in baza dreptului Uniunii sau a dreptului intern, care este proportional cu obiectivul urmarit, respecta esenta dreptului la protectia datelor si prevede masuri corespunzatoare si specifice pentru protejarea drepturilor fundamentale si a intereselor persoanei vizate.
Prelucrarea in alt scop	Art. 6 alin. (4): In cazul in care prelucrarea in alt scop decat cel pentru care datele cu caracter personal au fost colectate nu se bazeaza pe consimtamantul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, care constituie o masura necesara si proportionala intr-o societate democratica pentru a proteja obiectivele mentionate la art. 23 alin. (1), operatorul, pentru a stabili daca prelucrarea in alt scop este compatibila cu scopul pentru care datele cu caracter personal au fost colectate initial, ia in considerare, printre altele: (a) orice legatura dintre scopurile in care datele cu caracter personal au fost colectate si scopurile prelucrarii ulterioare preconizate; (b) contextul in care datele cu caracter personal au fost colectate, in special in ceea ce priveste relatia dintre persoanele vizate si operator; (c) natura datelor cu caracter personal, in special in cazul prelucrarii unor categorii speciale de date cu caracter personal, in conformitate cu art. 9, sau in cazul in care sunt prelucrate date cu caracter personal referitoare la condamnari penale si infractiuni, in conformitate cu art. 10; (d) posibilele consecinte asupra persoanelor vizate ale prelucrarii ulterioare preconizate; (e) existenta unor garantii adecvate, care pot include criptarea sau pseudonimizarea.

II. INFORMAREA PERSOANELOR VIZATE

Potrivit Articolelor 12-14 din GDPR, indiferent de temeiul prelucrarilor de date cu caracter personal, operatorii trebuie sa se conformeze unei obligatii specifice de informare a persoanelor vizate in legatura cu prelucrarile efectuate.

A. FORMA SI CONTINUTUL INFORMARII

Documentul de informare al persoanelor vizate cu privire la prelucrarile datelor lor cu caracter personal trebuie sa indeplineasca anumite cerinte formale si de continut.

A.1. Cum se face informarea persoanelor vizate?

Potrivit Art. 12 alin. (1) din GDPR, informarea trebuie oferita intr-o forma concisa, transparenta, inteligibila si usor accesibila, utilizand un limbaj clar si simplu.

Documentul de informare este pus la dispozitia persoanelor vizate in forme diferite, depinzand de scopurile prelucrarii si de sursa datelor (persoana vizata sau alta sursa): de exemplu, politica de confidentialitate a unui website, anexa la contractul incheiat cu persoana fizica, nota de informare inserata intr-un formular de aplicatie pentru o pozitie in cadrul operatorului, etc.

Ca principiu, nota de informare se livreaza in scris. Pot exista si informari verbale, la solicitarea persoanei vizate, cu conditia ca identitatea persoanei vizate sa fie dovedita prin alte mijloace.

Formele tipice de indeplinire a obligatiei de informare impuse de GDPR sunt:

(i) nota de informare / politica de confidentialitate inclusa in sau anexata la contract;
(ii) politica de confidentialitate pe website-ul companiei;
(iii) note de informare privind prelucrarea datelor angajatilor si a personalului auxiliar.

Nota de informare este necesara si in cazul clientilor persoane juridice. In acest caz, compania prelucreaza datele personale ale reprezentantilor sau imputernicitilor clientului, persoane fizice. In plus, cu ocazia primului contact cu aceste persoane fizice, furnizarea unei note de informare catre acestia este de asemenea necesara.

A.2. Ce contine informarea?

Depinzand de sursa de obtinere a datelor, respectiv persoana vizata insasi sau alte surse, informarea va avea un continut specific, reglementat de Art. 13 si 14 din GDPR. Prezentam mai jos principalele categorii de informatii care trebuie furnizate persoanei vizate:

a) Identitatea si datele de contact ale operatorului si ale reprezentantului acestuia;
b) Datele de contact ale responsabilului cu protectia datelor;
c) Scopurile in care sunt prelucrate datele cu caracter personal, precum si temeiul juridic al prelucrarii;
d) In cazul in care prelucrarea se face baza temeiului legitim, interesele legitime urmarite;

e) Categoriile de date cu caracter personal;
f) Destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
g) Informatii specifice privind transferurile de date personale in strainatate, daca exista o asemenea intentie;
h) Perioada pentru care vor fi stocate datele cu caracter personal sau, daca acest lucru nu este posibil, criteriile utilizate pentru a stabili aceasta perioada;
i) Existenta dreptului de a solicita operatorului, in ceea ce priveste datele cu caracter personal referitoare la persoana vizata, accesul la acestea, rectificarea sau stergerea acestora sau restrictionarea prelucrarii sau a dreptului de a se opune prelucrarii, precum si a dreptului la portabilitatea datelor;
j) Atunci cand prelucrarea are ca temei juridic consimtamantul persoanei vizate, existenta dreptului de a retrage consimtamantul in orice moment, fara a afecta legalitatea prelucrarii efectuate pe baza consimtamantului inainte de retragerea acestuia;
k) Dreptul de a depune o plangere in fata autoritatii de supraveghere;
l) Sursa din care provin datele cu caracter personal si, daca este cazul, daca acestea provin din surse disponibile public;
m) Daca furnizarea de date cu caracter personal reprezinta o obligatie legala sau contractuala sau o obligatie necesara pentru incheierea unui contract, precum si daca persoana vizata este obligata sa furnizeze aceste date cu caracter personal si care sunt eventualele consecinte ale nerespectarii acestei obligatii;
n) Existenta unui proces decizional automatizat incluzand crearea de profiluri, precum si, cel putin in cazurile respective, informatii pertinente privind logica utilizata si privind importanta si consecintele preconizate ale unei astfel de prelucrari pentru persoana vizata.

B. CAND SE FACE INFORMAREA?

In cazul datelor cu caracter personal colectate direct de la persoana vizata, informarea se face in momentul obtinerii datelor.

In cazul datelor cu caracter personal colectate din alte surse, informarea se face:

a) intr-un termen rezonabil dupa obtinerea datelor cu caracter personal, dar nu mai mare de o luna, tinandu-se seama de circumstantele specifice in care sunt prelucrate datele cu caracter personal;

b) daca datele cu caracter personal urmeaza sa fie utilizate pentru comunicarea cu persoana vizata, cel tarziu in momentul primei comunicari catre persoana vizata respectiva;

c) daca se intentioneaza divulgarea datelor cu caracter personal catre un alt destinatar, cel mai tarziu la data la care acestea sunt divulgate pentru prima oara.

C. EXCEPTII DE LA OBLIGATIA DE INFORMARE

Indiferent daca prelucrarile de date cu caracter personal sunt obtinute de la persoana vizata sau din alte surse, informarea nu este necesara daca si in masura in care persoana vizata detine deja informatiile respective.

In plus, pentru cazul particular al prelucrarilor de date cu caracter personal obtinute din alte surse, alte exceptii de la obligatia de informare pot deveni incidente:

a) in masura in care obligatia de informare este susceptibila sa faca imposibila sau sa afecteze in mod grav realizarea obiectivelor prelucrarii respective. In astfel de cazuri, operatorul ia masuri adecvate pentru a proteja drepturile, libertatile si interesele legitime ale persoanei vizate;

b) in cazul in care datele cu caracter personal trebuie sa ramana confidentiale in temeiul unei obligatii legale de a pastra secretul profesional.

D. CUM DOCUMENTAM INFORMAREA?

Un element intrinsec al obligatiei de informare care revine operatorului este documentarea indeplinirii obligatiei de informare sub toate aspecte sale:

(i) care a fost forma si continutul informarii furnizate persoanei vizate;
(ii) cand a fost furnizata informarea;
(iii) daca informarea nu a fost necesara, se va documenta motivul exceptarii.

Dovada indeplinirii obligatiei de informare, se poate face cu orice mijloc adecvat de proba, in functie de contextul concret, precum:

(i) corespondenta purtata cu clientul in faza pre-contractuala pe baza ofertei de colaborare (continand nota de informare / politica de confidentialitate);
(ii) semnatura a clientului pe contract (continand nota de informare / politica de confidentialitate);
(iii) semnatura a candidatului pe formularul de aplicatie (continand nota de informare) pentru o pozitie in cadrul operatorului sau pe nota de informare privind prelucrarea datelor angajatilor si a personalului auxiliar, etc.

III. DREPTURILE PERSOANELOR VIZATE

A. DREPTURI SPECIFICE INCIDENTE IN CONTEXTUL PRELUCRARILOR DATELOR CU CARACTER PERSONAL

GDPR prevede 8 drepturi specifice in materie de prelucrare a datelor cu caracter personal care pot fi exercitate in masura in care nu aduc atingere drepturilor si libertatilor altora:

a) Dreptul de acces la date;

b) Dreptul la rectificarea datelor;

c) Dreptul la stergerea datelor;

d) Dreptul la restrictionarea prelucrarii;

e) Dreptul la portabilitatea datelor;

f) Dreptul de opozitie la prelucrarea datelor;

g) Dreptul de a nu fi supus unor decizi automatizate, inclusiv profilarea;

h) Dreptul la notificarea destinatarilor privind rectificarea, stergerea ori restrictionarea datelor cu caracter personal.

Compania este tinuta in mod direct sa respecte drepturile specifice in materie de prelucrare a datelor cu caracter personal.

Raspunsul la cererile persoanelor vizate trebuie sa fie trimis in maximum o luna de la primirea acestora, cu posibilitatea prelungirii duratei cu maximum doua luni, daca vorbim despre o prelucrare complexa ori de un volum mare de astfel de cereri (in orice caz, inclusiv informarea cu privire la intarzierea unui raspuns ori refuzul de a lua masuri trebuie transmise in termenul de o luna).

Orice activitati desfasurate de companie pentru a raspunde solicitarilor persoanelor vizate trebuie sa fie desfasurate in mod gratuit, cu exceptia cazurilor in care solicitarile persoanelor vizate sunt excesive (ex. numar exagerat de solicitari identice, solicitari frecvente).

A.1. Dreptul de acces la baza de date si dreptul la informare

Compania are obligatia, la cererea transmisa pe orice canal de catre persoanele vizate (clienti, angajati, alte persoane fizice), de a le confirma acestora ce date prelucreaza si in ce conditii.

Persoanele vizate au dreptul de a obtine la cerere si in mod gratuit date referitoare la prelucrarile de date care le privesc, efectuate de catre societate, precum si dreptul de a obtine informatii privitoare la scopul prelucrarii, categoriile de date prelucrate, destinatarii datelor, perioada pentru care datele sunt stocate si drepturile de care beneficiaza in virtutea dispozitiilor legale in materie.

A.2. Dreptul la rectificarea datelor

Compania are obligatia de a asigura respectarea drepturilor persoanelor vizate de a obtine fara intarziere rectificarea oricaror date inexacte (eronate sau incomplete) care le privesc.

A.3. Dreptul la stergerea datelor

Persoanele vizate pot solicita companiei stergerea datelor care le privesc fara nicio intarziere.

Cand se aplica?

- datele cu caracter personal nu mai sunt necesare pentru indeplinirea scopurilor pentru

care au fost colectate sau prelucrate;

- persoana vizata isi retrage consimtamantul pe baza caruia are loc prelucrarea si nu exista niciun alt temei juridic pentru prelucrare;

- persoana vizata se opune prelucrarii si nu exista motive legitime care sa prevaleze in ceea ce priveste prelucrarea sau persoana vizata se opune prelucrarii in scopuri de marketing direct;

- datele cu caracter personal au fost prelucrate ilegal;

- datele cu caracter personal trebuie sterse pentru respectarea unei obligatii legale care revine companiei in temeiul dreptului Uniunii sau al dreptului intern sub incidenta caruia se afla aceasta.

Exceptii:

- atunci cand prelucrarea este necesara pentru exercitarea dreptului la libera exprimare si la informare;

- atunci cand prelucrarea este necesara pentru respectarea unei obligatii legale care prevede prelucrarea in temeiul dreptului Uniunii sau al dreptului intern care se aplica companiei sau pentru indeplinirea unei sarcini executate in interes public;

- atunci cand prelucrarea este necesara din motive de interes public in domeniul sanatatii publice;

- atunci cand prelucrarea este necesara in scopuri de arhivare in interes public, in scopuri de cercetare stiintifica sau istorica ori in scopuri statistice.

A.4. Dreptul la restrictionarea prelucrarii

Persoana vizata are dreptul de a obtine din partea companiei restrictionarea prelucrarii, respectiv limitarea acesteia (cu exceptia stocarii propriu-zise) strict la prelucrarile cu care persoana vizata este de acord si /sau strict la prelucrarile necesare in scopul constatarii, exercitarii sau apararii unui drept in instanta sau pentru protectia drepturilor unei alte persoane fizice sau juridice sau din motive de interes public al Uniunii sau al unui stat membru.

Restrictionarea se aplica atunci cand:

a) persoana vizata contesta exactitatea datelor, pentru o perioada care ii permite companiei sa verifice exactitatea datelor;
b) prelucrarea este ilegala, iar persoana vizata se opune stergerii datelor cu caracter personal, solicitand in schimb restrictionarea utilizarii lor;
c) compania nu mai are nevoie de datele cu caracter personal in scopul prelucrarii, dar persoana vizata I le solicita pentru constatarea, exercitarea sau apararea unui drept in instanta;
d) persoana vizata s-a opus prelucrarii pentru intervalul de timp in care se verifica daca drepturile legitime ale companiei prevaleaza asupra celor ale persoanei

vizate.

A.5. Dreptul la portabilitatea datelor

Dreptul la portabilitatea datelor implica obligatia companiei de a asigura:

(i) furnizarea datelor primite de la persoana vizata intr-un format accesibil la cererea acesteia;
(ii) transmiterea unor astfel de date catre alti operatori la cererea persoanei vizate, incidenta cand urmatoarele conditii cumulative sunt indeplinite:

a) prelucrarea se bazeaza pe consimtamant sau este necesara pentru executarea unui contract la care persoana vizata este parte sau pentru a face demersuri la cererea persoanei vizate inainte de incheierea unui contract;

b) este realizata prin mijloace automate (nu in forma fizica / hartie, ci prin orice mijloace automatizate).

A.6. Dreptul de opozitie la prelucrarea datelor

Persoanele vizate pot sa se opuna oricand la prelucrarea datelor lor cu caracter personal:
a) prelucrarilor efectuate in temeiul intereselor legitime urmarite de companie sau de o parte terta a datelor cu caracter personal, inclusiv crearii de profiluri.
b) fara motive si justificare, in cazul prelucrarii datelor in scopuri de marketing direct (ex. pentru promovarea serviciilor companiei).

Compania nu mai poate prelucra datele cu caracter personal in cazul opunerii, cu exceptia cazului in care demonstreaza ca are motive legitime si imperioase care justifica prelucrarea si care prevaleaza asupra intereselor, drepturilor si libertatilor persoanei vizate sau ca scopul prelucrarii este constatarea, exercitarea sau apararea unui drept in instanta.

A.7. Dreptul de a nu fi supus unor decizi automatizate, inclusiv profilarea

Persoanele vizate au dreptul ca datele lor cu caracter personal sa nu fie prelucrate in contextul luarii unor decizii automatizate.

Cand se aplica?

De regula, persoanele vizate au dreptul sa nu fie supuse unor decizii automatizate (fara implicarea factorului uman intr-o masura semnificativa) care produc efecte juridice (orice efecte produse din punct de vedere juridic asupra drepturilor legale ale persoanei vizate) ori efecte semnificative similare (influentarea altor drepturi/obligatii ale persoanelor vizate) asupra acestora.

Cand nu se aplica?

Prelucrarea datelor pentru luarea de decizii automatizate este permisa cand:

- este necesara pentru incheierea sau executarea unui contract intre persoana vizata si companie;

- este autorizata prin dreptul Uniunii sau dreptul intern care se aplica companiei si care prevede, de asemenea, masuri corespunzatoare pentru protejarea drepturilor, libertatilor si intereselor legitime ale persoanei vizate;

- persoana vizata si-a exprimat acordul explicit pentru o astfel de prelucrare.

A.8. Dreptul la notificarea destinatarilor privind rectificarea, stergerea ori restrictionarea datelor cu caracter personal

Compania are obligatia sa comunice fiecarui destinatar caruia i-au fost divulgate datele cu caracter personal ale persoanelor vizate orice rectificare sau stergere a datelor cu caracter personal sau restrictionare a prelucrarii efectuate.

O astfel de obligatie este incidenta cu exceptia cazului in care acest lucru se dovedeste imposibil sau presupune eforturi disproportionate. Compania are si obligatia de a informa persoana vizata cu privire la destinatarii respectivi daca aceasta solicita acest lucru.

B. MECANISME DE RASPUNS LA CERERILE DE EXERCITARE A DREPTURILOR PERSOANELOR VIZATE

Pentru a asigura tratarea cu celeritate a cererilor persoanelor vizate pentru exercitarea drepturilor specifice, urmatoarele mecanisme pot fi avute in vedere:

a) Alocarea unei/unor persoane care sa se ocupe de tratarea in timp util a cererilor persoanelor vizate, care sa raspunda in scris la asemenea solicitari;

b) Redactarea unor formulare de exercitare a drepturilor/raspuns tipizate care sa fie utilizate atunci cand clientii/angajatii/alte persoane vizate isi exercita drepturile specifice;

c) Daca cererile sunt transmise prin mijloace electronice, raspunsul trebuie transmis prin aceleasi mijloace, daca persoanele vizate nu solicita altfel;

d) Implementarea unor sectiuni specifice pentru exercitarea drepturilor persoanelor vizate online, in special in cazurile in care colectarea datelor se realizeaza online;

e) Pentru companiile cu personal numeros, conceperea unei proceduri specifice cu reguli clare de urmat in cazul primirii unor astfel de cereri, inclusiv cu principiile de avut in vedere in contextul conceperii raspunsurilor la cererile specifice.

C. EVIDENTA GESTIONARII CERERILOR DE EXERCITARE A DREPTURILOR PERSOANELOR VIZATE

Este recomandabila pastrarea de catre companie a unei evidente clare a raspunsurilor date in contextul cererilor persoanelor vizate de exercitare a drepturilor specifice in materie de prelucrare a datelor cu caracter personal.

Compania trebuie sa aiba dovezi clare scrise (inclusiv continand raspunsurile si data transmiterii acestora) care sa ateste indeplinirea obligatiilor specifice in materie; evidenta se poate pastra pe doua paliere: solicitari primite cu toate informatiile aferente cu evidentierea datei primirii acestora si respectiv raspunsuri transmise, cu evidentierea datei transmiterii raspunsurilor, iar unde este cazul de prelungire a termenului de raspuns dupa o luna, cu indicarea clara a motivului prelungirii.

Este preferabila pastrarea dovezilor in forma scrisa. Cu toate acestea, daca persoana vizata solicita anumite informatii oral, este admisibila si pastrarea unor dovezi ale inregistrarilor care sa ateste raspunsul acordat unor asemenea solicitari.

IV. EVIDENTELE OPERATIUNILOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

A. ANALIZA INCIDENTEI OBLIGATIEI DE MENTINERE A EVIDENTELOR PRELUCRARILOR

Din interpretarea art. 30, para. 5 din Regulament, rezulta ca obligatia mentinerii unei evidente a activitatilor de prelucrare a datelor cu caracter personal incumba, de principiu, intreprinderilor sau organizatiilor cu peste 250 de angajati.

Intreprinderile sau organizatiile cu mai putin de 250 de angajati sunt tinuti de aceasta obligatie doar daca ”*prelucrarea pe care o efectueaza este susceptibila sa genereze un risc pentru drepturile şi libertaţile persoanelor vizate, prelucrarea nu este ocazionala sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnari penale şi infracţiuni, astfel cum se menţioneaza la articolul 10*”.

B. FORMA SI CONTINUTUL EVIDENTEI PRELUCRARII DATELOR

Conform dispozitiilor Art. 30 din Regulament, fiecare operator si, dupa caz, reprezentantul acestuia pastreaza o evidenta a activitatilor de prelucrare desfasurate sub responsabilitatea lor.

Evidenta mentinuta de operatori si, dupa caz, de reprezentantii acestora trebuie sa cuprinda urmatoarele informatii:

a) numele si datele de contact ale operatorului si, dupa caz, ale operatorului asociat, ale reprezentantului operatorului si ale responsabilului cu protectia datelor;

b) scopurile prelucrarii;

c) o descriere a categoriilor de persoane vizate si a categoriilor de date cu caracter personal;

d) categoriile de destinatari carora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din tari terte sau organizatii internationale;

e) daca este cazul, transferurile de date cu caracter personal catre o tara terta sau o organizatie internationala, inclusiv identificarea tarii terte sau a organizatiei internationale respective si, in cazul transferurilor mentionate la articolul 49 alineatul (1) al doilea paragraf, documentatia care dovedeste existenta unor garantii adecvate;

f) acolo unde este posibil, termenele-limita preconizate pentru stergerea diferitelor categorii de date;

g) acolo unde este posibil, o descriere generala a masurilor tehnice si organizatorice de securitate mentionate la articolul 32 alineatul (1).

Aceasta lista reprezinta un cumul de cerinte minime obligatorii ce trebuie respectate si integrate in registrul de evidenta de catre compania ce desfasoara in mod sistematic activitati de prelucrare a datelor cu caracter personal.

V. RESPONSABILUL PENTRU PROTECTIA DATELOR CU CARACTER PERSONAL (DPO)

A. PUNCTE CHEIE

a) Este responsabilitatea companiei sa evalueze necesitatea numirii unui DPO in cadrul organizatiei, prin raportare la criteriile impuse de Regulament;

b) Este recomandabil sa fie documentata in scris aceasta evaluare, ca parte a proiectului de conformare Regulament si sa actualizeze periodic evaluarea facuta;

c) DPO in cadrul companiei trebuie sa indeplineasca toate sarcinile si sa se bucure de toate garantiile pentru a isi desfasura activitatea in parametrii reglementati de Regulament;

e) Numirea voluntara de DPO este o recomandare de buna practica. Daca compania nu numeste DPO trebuie sa acorde atentie tuturor celorlalte aspecte de conformare aplicabile.

B. CAND ESTE OBLIGATORIU CA O COMPANIE SA NUMEASCA DPO?

B.1. Norma juridica relevanta

Art. 37 alin. (1) din Regulament stabileste situatiile in care este obligatorie numirea DPO:

a) prelucrarea este efectuata de o autoritate sau un organism public, cu exceptia instantelor care actioneaza in exercitiul functiei lor jurisdictionale;

b) activitatile principale ale operatorului sau persoanei imputernicite constau in operatiuni de prelucrare care, prin natura, domeniul de aplicare si/sau scopurile lor, necesita o monitorizare periodica si sistematica a persoanelor vizate pe scara larga;

c) activitatile principale ale operatorului sau ale persoanei imputernicite de operator constau in prelucrarea pe scara larga a unor categorii speciale de date sau a unor date cu caracter personal privind condamnari penale si infractiuni.

B.2. Clarificari conceptuale

Fiecare companie va trebui sa evalueze daca, prin raportare la propria sa organizare si activitate, se incadreaza in vreuna dintre variantele de mai sus.

Cateva elemente-cheie trebuie avute in vedere pentru aceasta evaluare:

a) Conceptul de „*activitati principale*”

Potrivit A29 GL, activitati principale inseamna „*operatiuni-cheie pentru atingerea scopurilor operatorului / persoanei imputernicite*”, fara a exclude insa „*activitatile in care prelucrarea datelor cu caracter personal este o parte inextricabila a activitatii operatorului / persoanei imputernicite”*.

b) Conceptul de „*prelucrare pe scara larga*”

Regulamentul nu ofera criterii precise pentru a valida acest element. A29 GL ofera o serie de criterii orientative de care trebuie tinut cont in calificarea unei prelucrari ca fiind „*pe scara larga*”: numarul de persoane vizate / proportia din populatia relevanta, volumul si varietatea datelor personale prelucrate, durata prelucrarii, intinderea geografica.

c) Conceptul de „*monitorizare periodica si sistematica*”

Conform A29 GL,

(i) *monitorizare* inseamna orice forma de urmarire si profilare in mediu online, dar nu sunt excluse si forme de monitorizare „clasica”;

(ii) *periodica* inseamna in principiu, fie continua, fie repetata la intervale fixe de timp;

(iii) *sistematica* inseamna in principiu realizata pe baza unui sistem, pre-aranjata, organizata sau metodica, fiind realizata ca parte a unui plan general sau strategie de

colectare de date.

d) Conceptul de „*categorii speciale de date”*

Acesta include categoriile de date stabilite prin art. 9 din Regulament: *originea rasiala sau etnica, opiniile politice, confesiunea religioasa sau convingerile filozofice sau apartenenta la sindicate si prelucrarea de date genetice, de date biometrice pentru identificarea unica a unei persoane fizice, de date privind sanatatea sau de date privind viata sexuala sau orientarea sexuala ale unei persoane fizice*.

La acestea, se adauga *datele cu caracter personal privind condamnari penale si infractiuni*, mentionate la art. 10 din Regulament.

B.3. Concluzii

Avand in vedere prevederile Regulamentului si precizarile A29 GL, fiecare companie va trebui sa evalueze necesitatea sau oportunitatea numirii unui DPO, prin raportare la dimensiunea sa, modul de organizare, tipurile de prelucrari de date cu caracter personal, volumul si varietatea acestora, durata prelucrarii si stocarii de date, aria geografica acoperita.

C. SARCINILE DPO

Ca principiu, DPO trebuie sa aiba o implicare efectiva si la timp in toate aspectele privind protectia datelor din cadrul organizatiei.

Principalele sarcini ale unui DPO sunt urmatoarele:

La preluarea mandatului

a) Auditarea organizatiei cu relevarea situatiei existente si vulnerabilitatile de conformitate identificate:

(i) Colecteaza informatii privind activitatile de prelucrare desfasurate;

(ii) Munca colaborativa cu personalul din departamentele relevante;

b) Consiliaza conducerea companiei cu privire la obligatiile specifice si vulnerabilitatile identificate;

c) Coordoneaza planuri pentru implementarea in organizatie a cerintelor Regulamentului si conformare continua;

d) Training pentru management si salariati privind obligatiile specifice domeniului.

Dezvoltare si mentenanta

a) Redacteaza documentatia specifica:

b) Evidenta activitatilor de prelucrare;

c) Evaluarea impactului asupra protectiei datelor (DPIA);

d) Proceduri interne (e.g. securitatea datelor (clean desk policy), monitorizare acces, corespondenta electronica, gestionare incidente de securitate);

e) Monitorizeaza activitatile organizatiei si faciliteaza conformarea incepand cu momentul conceperii si in mod implicit (protectia datelor by design si by default);

f) Asistenta in cazul survenirii unui incident de securitate.

Altele

a) DPO este punct de contact pentru persoanele vizate;

b) DPO este punct de contact si cooperare cu autoritatea de supraveghere.

D. INTEGRAREA DPO IN ORGANIZATIE

Regulamentul impune o serie de garantii pe care organizatia trebuie sa le ofere DPO in vederea indeplinirii sarcinilor si rolului acestuia:

1. Implicare in toate aspectele privind protectia datelor

a) DPO participa cu regularitate la sedintele managementului;
b) Recomandarile DPO trebuie luate in considerare (A29 GL recomanda documentarea motivelor pentru care nu este respectata opinia DPO);
c) Consultare in cazul aparitiei unui incident de securitate.

2. Asigurarea resurselor necesare pentru indeplinirea sarcinilor

a) Compania trebuie sa asigure ca DPO dispune de resursele de timp necesare indeplinirii sarcinilor sale (in special pentru DPO intern care cumuleaza si alte atributii);
b) Suport adecvat la resurse financiare, infrastructura (locatie, facilitati, echipamente), inclusiv personal;
c) Drept de acces la toate datele cu caracter personal;
d) Relationare cu departamentele companiei (resurse umane, legal, IT, marketing);
e) Training DPO pentru perfectionare continua.

3. Independenta DPO

a) DPO „lucreaza" in primul rand pentru persoanele vizate si doar in subsidiar pentru organizatie;

b) Orice relatie de subordonare ierarhica este inaplicabila in cazul DPO;
c) DPO nu vor primi instructiuni despre cum sa abordeze o problema de conformitate, cum sa investigheze un anumit incident;
d) DPO nu are putere de decizie, dar este un consultant a carui opinie trebuie ascultata la cel mai inalt nivel de management.

4. Stabilitate (nu poate fi sanctionat sau demis pentru indeplinirea sarcinilor)

a) O opinie "incomoda" nu poate constitui temei al demiterii sau sanctionarii (sau al incetarii contractului cu DPO extern);
b) Sanctiunile sunt de asemenea interzise (refuz la promovare, bonusuri, amenintare);
c) DPO poate fi demis / sanctionat pentru neindeplinirea sarcinilor conform regulilor comune aplicabile oricarui alt angajat / colaborator (abatere grava, abateri repetate, necorespundere profesionala, neindeplinirea obligatiilor contractuale).

5. Pozitia de DPO nu trebuie sa genereze un conflict de interese

a) In principiu, DPO nu poate exercita o functie care ii permite sa determine scopurile sau mijloacele unei prelucrari;
b) DPO este incompatibil cu o pozitie de conducere / de decizie.

Buna-practica pentru evitarea conflictului de interese:
a) Identificarea in organizatie a pozitiilor incompatibile cu DPO;
b) Proceduri interne de evitare / rezolvare a conflictului;
c) Declaratie formala ca DPO nu se afla in pozitie de conflict (la momentul notificarii catre autoritatea de supraveghere).

Societatea va contracta o persoana juridica autorizata, avand toate certificarile privind protectia datelor cu caracter personal, pentru a exercita functia de responsabil cu protectia datelor cu caracter personal pentru aceasta.

VI. EVALUAREA IMPACTULUI ASUPRA PROTECTIEI DATELOR (DPIA)

A. CONCEPT

Conform art. 35 para. 1 din Regulament, „*avand in vedere natura, domeniul de aplicare, contextul si scopurile prelucrarii, in cazul in care un tip de prelucrare, in special cel bazat pe utilizarea noilor tehnologii, este susceptibil sa genereze un risc ridicat pentru drepturile si libertatile persoanelor fizice, operatorul efectueaza, inaintea prelucrarii, o evaluare a impactului operatiunilor de prelucrare prevazute asupra protectiei datelor cu caracter personal. O evaluare unica poate aborda un set de operatiuni de prelucrare similare care prezinta riscuri ridicate similare.*"

Astfel, principalele coordonate ale DPIA sunt urmatoarele:

a) Obligativitatea DPIA intervine atunci cand prelucrarea, in special cea bazata pe noile tehnologii, este susceptibila sa genereze un risc ridicat pentru drepturile si libertatile persoanelor fizice.

b) O evaluare unica poate fi utilizata pentru analiza unor operatiuni de procesare multiple care prezinta similitudini din perspectiva riscului generat;

c) Evaluarea trebuie realizata anterior prelucrarii datelor cu caracter personal.

In analiza riscului major, relevant este si numarul persoanelor vizate.

Daca, in urma analizei, se constata ca operatiunea de procesare este susceptibila sa genereze un risc ridicat, operatorul trebuie:

a) Fie sa adopte o metodologie DPIA care indeplineste criteriile din Regulament si din ”Ghidul privind Evaluarea impactului asupra protectiei datelor (DPIA) si stabilirea daca o prelucrare este „susceptibila sa genereze un risc ridicat” in sensul Regulamentului 2016/679” emis de catre A29 GL (”Ghidul A29 GL privind DPIA”) fie sa implementeze un proces DPIA sistematic care:

(i) Indeplineste conditiile din Anexa nr. 2 din Ghidul A29 GL privind DPIA;

(ii) Este integrat in procesele existente de dezvoltare si revizuire operationala si de risc in conformitate cu procesele interne, contextul si cultura organizationala;

(iii) Implica persoanele interesate relevante si le defineste atributiile intr-un mod clar (operator, DPO, persoane vizate, persoana imputernicita etc).

b) Sa transmita raportul DPIA catre autoritatea de supraveghere competenta atunci cand i se solicita aceasta;

c) Sa consulte autoritatea de supraveghere atunci cand nu au reusit sa determine masuri suficiente pentru prevenirea riscului ridicat;

d) Sa revizuiasca periodic DPIA si procedurile aferente:

e) Sa documenteze deciziile luate.

B. RECOMANDARI PRIVIND MODUL DE REALIZARE A DPIA

In cazul in care nu este clar daca si in ce masura PIA este necesara, A29 GL recomanda ca entitatile vizate sa desfasoare DPIA intrucat aceasta procedura reprezinta un instrument util pentru operatori si persoanele imputernicite in executarea obligatiilor ce le revin in baza legislatiei de protectie a datelor cu caracter personal.

Obligativitatea parcurgerii DPIA intervine in cazul operatiunilor de procesare ce indeplinesc criteriile din art. 35 GDPR si care sunt initiate dupa data de 25 mai 2018. Cu toate acestea, A29 GL recomanda parcurgerea acestei proceduri si pentru operatiunile de procesare in desfasurare la data de 25 mai 2018. In plus, ”*acolo unde este necesar, operatorul efectueaza o analiza pentru a evalua daca prelucrarea are loc in conformitate*

cu evaluarea impactului asupra protectiei datelor, cel putin atunci cand are loc o modificare a riscului reprezentat de operatiunile de prelucrare".

Art. 35 para. 7 din Regulament enunta o serie de elemente cu caracter minimal ce trebuie incluse in DPIA:

a) "*o descriere sistematica a operatiunilor de prelucrare preconizate si a scopurilor prelucrarii, inclusiv, dupa caz, interesul legitim urmarit de operator;*

b) o evaluare a necesitatii si proportionalitatii operatiunilor de prelucrare in legatura cu aceste scopuri;

c) o evaluare a riscurilor pentru drepturile si libertatile persoanelor vizate; si

d) *masurile preconizate in vederea abordarii riscurilor, inclusiv garantiile, masurile de securitate si mecanismele menite sa asigure protectia datelor cu caracter personal si sa demonstreze conformitatea cu dispozitiile prezentului regulament, luand in considerare drepturile si interesele legitime ale persoanelor vizate si ale altor persoane interesate.*"

Anexa nr. 2 din Ghidul A29 GL privind DPIA stabileste o serie de criterii comune care clarifica cerintele minimale ale Regulamentului, oferind in acelasi timp suficienta libertate in implementarea acestuia.

In acelasi timp, A29 GL incurajeaza dezvoltarea unor proceduri specifice fiecarui sector de activitate.

In plus, DPIA trebuie publicata, in tot sau in parte si trebuie comunicata autoritatii cu competenta in domeniu, in speta Autoritatii Naţionale de Supraveghere a Prelucrarii Datelor cu Caracter Personal. Publicarea nu este o cerinta legala impusa de Regulament, dar intareste increderea persoanelor vizate in operatorul de date si il ajuta pe acesta din urma sa demonstreze respectarea principiilor responsabilitatii si transparentei.

VII. CONFIDENTIALITATEA SI SECURITATEA DATELOR

A. ASPECTE GENERALE PRIVIND CONFIDENTIALITATEA SI SECURITATEA DATELOR

Conform art. 32 din Regulament, *"Avand in vedere stadiul actual al dezvoltarii, costurile implementarii si natura, domeniul de aplicare, contextul si scopurile prelucrarii, precum si riscul cu diferite grade de probabilitate si gravitate pentru drepturile si libertatile persoanelor fizice, operatorul si persoana imputernicita de acesta implementeaza masuri tehnice si organizatorice adecvate in vederea asigurarii unui nivel de securitate corespunzator acestui risc, incluzand printre altele, dupa caz:*

a) pseudonimizarea si criptarea datelor cu caracter personal;

b) capacitatea de a asigura confidentialitatea, integritatea, disponibilitatea si rezistenta continue ale sistemelor si serviciilor de prelucrare;

c) capacitatea de a restabili disponibilitatea datelor cu caracter personal si accesul la acestea in timp util in cazul in care are loc un incident de natura fizica sau tehnica;

d) un proces pentru testarea, evaluarea si aprecierea periodice ale eficacitatii masurilor tehnice si organizatorice pentru a garanta securitatea prelucrarii".

Un rol important in evaluarea nivelului adecvat de securitate il vor avea riscurile pe care le implica prelucrarea, riscuri ce pot fi generate, accidental ori ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizata sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate intr-un alt mod.

Demonstrarea indeplinirii conditiilor mentionate se poate realiza, printre altele, prin aderarea la un cod de conduita aprobat in temeiul art. 40 din Regulament sau la un mecanism de certificare aprobat in temeiul art. 42 GDPR.

B. DEZVALUIRI DE DATE LA SOLICITAREA AUTORITATILOR PUBLICE

Art. 6 para. 1 lit. c) din Regulament prevede ca prelucrarea datelor cu caracter personal este legala daca, printre altele, "*prelucrarea este necesara in vederea indeplinirii unei obligatii legale care ii revine operatorului*".

Ca atare, companiile pot transmite date cu caracter personal pe care le prelucreaza ca operatori catre autoritati publice doar daca si in masura in care, *in principal*:

a) Aceasta se manifesta intr-o obligatie legala pentru acestea;

b) Autoritatea care solicita aceste informatii are competenta in domeniu, verificata in prealabil de catre compania careia i se solicita transferul;

c) Compania asigura un nivel de protectie adecvat al datelor prelucrate si astfel transmise;

d) Transferul se realizeaza cu respectarea principiilor prevazute de GDPR si sintetizate in art. 5 din acesta: legalitate, echitate si transparenta; principiul limitarii transferului in functie de scop; principiul reducerii la minimum a datelor transferate; principiul exactitatii datelor; principiul limitarii legate de stocarea datelor; principiul asigurarii integritatii si confidentialitatii datelor; principiul responsabilitatii.

VIII. BRESELE DE SECURITATE

Conform art. 5 din Regulament, unul dintre principiile de baza care guverneaza prelucrarea datelor cu caracter personal este acela ca datele trebuie sa fie prelucrate intr-un mod care asigura securitatea adecvata a acestora. Garantiile legale ale acestui principiu se regasesc in principal in art. 32-34 din Regulament.

Companiile sunt obligate sa implementeze masuri tehnice si organizatorice adecvate in vederea asigurarii unui nivel de securitate corespunzator (art. 32 din Regulament). Companiile trebuie sa stabileasca masurile necesare si suficiente pentru a asigura securitatea datelor (componenta preventiva a politicilor interne privind securitatea datelor).

Totodata, chiar daca art. 33 din Regulament nu o prevede in mod expres, companiile trebuie sa implementeze masuri tehnice si organizatorice care, in cazul aparitiei unei brese de securitate, asigura componenta reactiva a politicilor interne privind securitatea datelor. Aceste masuri trebuie sa ajute operatorul:

a) sa stabileasca imediat daca s-a produs o bresa de securitate (preambul, pct. 87 din Regulament);

b) daca este cazul, sa notifice autoritatea de supraveghere a prelucrarii datelor cu caracter personal (art. 33 din Regulament);

c) dupa caz, sa informeze persoana sau persoanele vizate afectate de aparitia bresei de securitate (art. 34 din Regulament).

Nu in ultimul rand, incidentele de securitate trebuie documentate conform art. 33 alin. (5) din Regulament.

Art. 4 alin. (12) din Regulament defineste bresa de securitate: *„o incalcare a securitatii care duce, in mod accidental sau ilegal, la distrugerea, pierderea, modificarea sau divulgarea neautorizata a datelor cu caracter personal (...) sau la accesul neautorizat la acestea”*.

In Ghidul privind notificarea incalcarii securitatii datelor, A29 GL explica notiunile de „distrugere”, „pierdere”, „modificare” si „divulgare neautorizata”:

a) „distrugerea” se refera la situatia in care datele nu mai exista ori nu mai exista intr-o forma care sa le faca utilizabile de catre operatori;

b) „pierderea” are in vedere situatia in care datele pot sa existe, insa operatorul a pierdut controlul sau accesul la date;

c) „modificarea” desemneaza situatia in care datele sunt corupte sau modificate in alt mod, astfel incat ele nu mai sunt complete;

d) in fine, „divulgarea neautorizata” are in vedere situatia in care datele au fost transmise catre ori accesate de catre persoane neautorizate sa primeasca sau sa acceseze datele personale.

Privind notiunea de bresa de securitate prin prisma celor trei elemente ale securitatii datelor (disponibilitate, integritate, confidentialitate), rezulta ca exista o bresa de securitate atunci cand:

a) datele devin indisponibile ca urmare a:

(i) distrugerii;

(ii) pierderii accesului;

b) este afectata integritatea datelor prin modificarea acestora;

c) este compromisa confidentialitatea datelor prin:

(i) divulgarea neautorizata;

(ii) accesul neautorizat la date.

Exemple de brese de securitate:

- atacuri informatice tip ransomware,

- pierderea cheii de criptare a datelor,

- nefunctionarea sistemelor informatice,

- pierderea unor documente,

- transmiterea unei corespondente la adresa gresita etc.

Bresele de securitate pot avea cauze diferite: de la nefunctionarea sau functionarea necorespunzatoare a sistemelor informatice pana la erori umane.

Pentru aceasta, compania va asigura instruirea persoanelor implicate in procesele de prelucrare a datelor astfel incat acestea sa poata identifica bresele de securitate si sa le aduca la cunostinta persoanelor responsabile pentru a lua masurile necesare in vederea analizei si limitarii consecintelor bresei de securitate si, dupa caz, in vederea notificarii autoritatii de supraveghere si eventual a persoanelor vizate.

A. NOTIFICAREA AUTORITATII DE SUPRAVEGHERE

Art. 33 din Regulament reglementeaza obligatia operatorului de a notifica bresele de securitate catre autoritatea de supraveghere a prelucrarii datelor cu caracter personal.

Scopul notificarii autoritatii este ca aceasta sa poata interveni pentru limitarea riscurilor asupra drepturilor si libertatilor persoanelor vizate.

Nu orice bresa de securitate trebuie notificata autoritatii de supraveghere. Conform art. 32 din Regulament, nu este obligatorie notificarea daca respectiva bresa nu este susceptibila sa genereze un risc pentru drepturile si libertatile persoanelor vizate. Este obligatia operatorului sa analizeze daca incidentul de securitate cu care se confrunta genereaza

riscuri pentru drepturile si libertatilor persoanelor vizate. Analiza se face de la caz la caz, pe baza urmatoarelor elemente:

a) tipul incidentului;

b) natura, contextul, volumul datelor afectate;

c) posibilitatea de a identifica persoanele vizate;

d) consecintele incidentului asupra persoanelor vizate;

e) circumstantele persoanelor vizate;

f) circumstantele operatorului in cauza (exemplu: pierderea unor date cu caracter personal criptate cu un algoritm de criptare complex nu este susceptibila sa genereze riscuri pentru drepturile si libertatile persoanelor vizate, atat timp cat criptarea asigura ca datele nu pot fi accesate de persoane neautorizate; totusi, daca datele nu sunt criptate, pierderea acestora ar trebui notificata).

In cazurile in care notificarea autoritatii este obligatorie, aceasta trebuie facuta „fara intarziere", de principiu nu mai tarziu de 72 de ore de la data la care operatorul a luat cunostinta de existenta bresei.

Continutul minim al notificarii este reglementat de art. 33 din Regulament. La pregatirea notificarii, compania va trebui sa protejeze confidentialitatea informatiilor oferite de clienti, sens in care vor oferi autoritatii detalii despre categoriile si numarul persoanelor afectate, fara insa a compromite confidentialitatea datelor primite de la clienti. In anumite situatii, este posibil ca nu toate datele sa fie de la inceput la dispozitia operatorului, unele amanunte devenind disponibile pe masura ce operatorul investigheaza bresa. Pentru aceste situatii, Regulamentul (art. 33 alin. (4)) si A29 GL recunosc posibilitatea notificarii etapizate, in care operatorul transmite autoritatii de supraveghere datele relevante pe masura ce acestea devin disponibile.

B. INFORMAREA PERSOANELOR VIZATE

Art. 34 din Regulament reglementeaza obligatia operatorului de a informa persoanele vizate cu privire la bresele de securitate. Scopul informarii este ca persoanele vizate sa isi poata lua masuri de protectie.

Informarea persoanelor vizate este obligatorie numai daca incidentul de securitate este susceptibil sa genereze un risc ridicat pentru drepturile si libertatile persoanelor vizate. Daca notificarea autoritatii de supraveghere este obligatorie ori de cate ori exista un risc privind drepturile si libertatile persoanelor vizate, informarea persoanelor vizate este obligatorie atunci cand exista un risc *ridicat* pentru drepturile si libertatile acestora.

Regulamentul nu prevede criterii obiective in functie de care se determina nivelul riscului generat de incidentul de securitate. Conform Ghidului privind notificarea incalcarii

securitatii datelor, la analiza nivelului de risc, operatorul va avea in vedere criteriile de mai jos:

a) tipul incidentului;

b) natura, contextul, volumul datelor afectate;

c) posibilitatea de a identifica persoanele vizate;

d) consecintele incidentului asupra persoanelor vizate;

e) circumstantele persoanelor vizate;

f) circumstantele operatorului in cauza;

g) numarul persoanelor afectate.

In cazurile in care informarea persoanelor vizate este obligatorie, aceasta trebuie facuta „fara intarziere". Continutul notificarii este reglementat de art. 34 din Regulament.

Regulamentul nu prescrie un anume formalism pentru informarea persoanelor vizate. Daca circumstantele concrete nu reclama o alta abordare, informarea se va face printr-o comunicare adresata direct persoanei vizate, printr-un mijloc de comunicare corespunzator (posta electronica, SMS etc.). Cu titlu de exceptie, doar in situatia in care contactarea directa a persoanei/persoanelor vizate ar presupune un efort disproportionat, se poate face o informare publica.

C. EVIDENTA BRESELOR DE SECURITATE

Toate incidentele de securitate trebuie documentate. Obligatia de a documenta incidentele de securitate se intinde si asupra acelor incidente care nu au facut obiectul notificarii.

Regulamentul nu prevede o forma anume a instrumentului care documenteaza bresele de securitate. Totusi, continutul acestuia este reglementat in art. 33 alin. (5) din Regulament. In cazul incidentelor de securitate pentru care s-a luat decizia sa nu se notifice autoritatea de supraveghere sau persoanele vizate, operatorul va face mentiune despre decizia de a nu notifica, aratand motivele care au fundamentat aceasta decizie.

IX. STOCAREA DATELOR CU CARACTER PERSONAL

A. ASPECTE GENERALE

Datele cu caracter personal trebuie sa fie pastrate pe o perioada care nu depaseste perioada necesara prelucrarii pentru scopul identificat. Principiul stocarii limitate a datelor cu caracter personal deriva din urmatoarele principii:

- datele cu caracter personal trebuie sa fie adecvate, relevante si neexcesive;

- datele cu caracter personal trebuie sa fie exacte si actualizate.

In mod evident, datele cu caracter personal stocate pentru perioade mai lungi decat cele necesare prelucrarii pentru scopul identificat vor deveni in mod automat excesive. Totodata, ele ar putea deveni nerelevate si chiar inexacte.

Regulamentul nu stabileste perioada standard de stocare a datelor cu caracter personal si nici reguli detaliate care sa ajute operatorii ori persoanele imputernicite sa stabileasca aceasta perioada. Revine asadar companiei sarcina sa stabileasca perioadele de retinere a datelor cu caracter personal prelucrate.

In contextul prelucrarii datelor cu caracter personal, pentru a se conforma regulilor privind retentia datelor, compania va implementa doua tipuri de reguli interne:

a) politici de arhivare, in baza carora datele cu caracter personal care nu sunt prelucrate in activitatea curenta, dar pentru retinerea carora exista o justificare, sa fie arhivate cu respectarea garantiilor privind securitatea datelor;

b) politici de stergere, in baza carora se vor revizui datele cu caracter personal prelucrate si se vor sterge, sau, dupa caz, se vor anonimiza acele date cu caracter personal de care nu mai este nevoie.

Durata prelucrarii datelor cu caracter personal este specifica fiecarui tip de prelucrare, tinand seama de considerentele mentionate mai sus, precum si pentru indeplinirea unor obligatii legale (fiscale, arhivare etc.).

In scopul limitarii prelucrarii, societatea va efectua periodic o revizuire a necesitatii de prelucrare a datelor, pentru a limita cat mai mult posibil sfera datelor supuse prelucrarii.
Societatea va lua toate masurile necesare pentru pastrarea datelor cu caracter personal de o maniera exacta, completata si actualizata, pentru a indeplini scopurile pentru care acestea au fost colectate. Datele inexacte sau incomplete vor fi rectificate sau eliminate din evidenta curenta.
Datele cu caracter personal vor fi pastrate numai pe perioada necesara indeplinirii scopurilor stabilite, cu respectarea drepturilor persoanei vizate, in special a dreptului de acces, de interventie si de opozitie.
In urma verificarilor periodice, datele cu caracter personal detinute de operator care nu mai servesc realizarii scopurilor sau indeplinirii unor obligatii legale, vor fi distruse sau transformate in date anonime intr-un interval de timp rezonabil, potrivit procedurilor stabilite de lege.

Cu titlu de exemplu, art. 25 din Legea nr. 82/1991 – Legea contabilitatii prevede urmatoarele:

“(1) Registrele de contabilitate obligatorii şi documentele justificative care stau la baza inregistrărilor in contabilitatea financiară se păstrează in arhiva persoanelor prevăzute la art. 1 ***timp de 10 ani,*** *cu incepere de la data incheierii exerciţiului financiar in cursul*

căruia au fost intocmite, cu excepţia statelor de salarii, care se păstrează ***timp de 50 de ani.***
(2) Prin excepţie de la prevederile alin. (1) se pot stabili, in mod justificat, prin ordin al ministrului economiei şi finanţelor , registrele de contabilitate şi documentele justificative care se păstrează ***timp de 5 ani****."*

Inregistrarile de supraveghere si protectie video nu trebuie, in principiu, sa fie stocate mai mult de **o luna**.

Datele cu caracter personal referitoare la clienti nu trebuie sa fie stocate mai mult de **trei ani** de la sfarsitul relatiei contractuale.

B. POLITICI DE ARHIVARE

Scopul politicilor de arhivare va fi acela de a asigura un flux corespunzator al lucrarilor inactive si al datelor cu caracter personal din acestea.

Important, datele cu caracter personal arhivate nu au un regim juridic derogatoriu, acestora aplicandu-li-se toate prevederile privind prelucrarea datelor cu caracter personal. Spre pilda, compania va trebui sa dea curs unei solicitari prin care se exercita dreptul de acces, chiar daca datele vizate prin cerere vor fi fost arhivate.

C. POLITICI DE STERGERE

Scopul politicilor de stergere va fi acela de a stabili, pentru fiecare categorie de date cu caracter personal, perioada de stocare si procedura ce urmeaza a fi aplicata dupa expirarea acestei perioade – stergerea definitiva sau, dupa caz, anonimizarea.

La stabilirea perioadelor de retentie se vor avea in vedere in primul rand prevederile din legislatie privind stocarea datelor. Datele nu vor fi stocate pentru perioade mai lungi decat perioada legala.

Acolo unde nu exista termene de stocare a datelor stabilite in actele normative, compania va stabili perioadele de stocare a datelor cu caracter personal tinand cont de scopul prelucrarii datelor personale si de contextul prelucrarii acestora.

Perioada de retentie a datelor cu caracter personal trebuie stabilita de la caz la caz, in functie de scopul pentru care au fost colectate respectivele date. Astfel, odata ce datele nu mai sunt necesare scopului pentru care au fost colectate, acestea vor fi sterse sau anonimizate.

De exemplu, atunci cand contractul semnat cu persoana vizata inceteaza, compania va trebui sa analizeze care sunt datele de care nu mai are nevoie (acestea urmand a fi sterse sau anonimizate) respectiv care sunt datele care trebuie mentinute in continuare, in ce scop si pentru cat timp. La incetarea contractului, compania va trebui sa retina in continuare date cu caracter personal pentru a raspunde eventualelor plangeri sau pretentii ale clientului. Cum am aratat mai sus, aceste date ar trebui pastrate in arhiva companiei

pentru o perioada suficienta astfel ca dupa trecerea acestei perioade, formularea unei plangeri sau a unei pretentii in legatura cu prestatia companiei sa nu mai fie posibila.

X. TRANSFERUL DATELOR CU CARACTER PERSONAL CATRE STATE TERTE

A. CONCEPT SI DELIMITARE

Conform art. 45 para. 1 din Regulament, „*transferul de date cu caracter personal catre o tara terta sau o organizatie internationala se poate realiza atunci cand Comisia a decis ca tara terta, un teritoriu ori unul sau mai multe sectoare specificate din acea tara terta sau organizatia internationala in cauza asigura un nivel de protectie adecvat. Transferurile realizate in aceste conditii nu necesita autorizari speciale*". Decizia Comisiei in acest sens este obligatorie pentru toate statele membre UE.

In cazul in care este necesar sa se predea si sa se prelucreze datele personale ale persoanelor vizate intr-un stat din afara Uniunii Europene, societatea se va asigura ca procesarea de date cu caracter personal este conforma cerintelor de securitate la care sunt supuse procesarile din cadrul Comunitatii Europene, a caror componenta o reprezinta respectarea standardelor UE privind prelucrarea datelor personale, asigurand astfel indeplinirea dezideratelor prevazute de legislatia in materie de protectie a datelor cu caracter personal.

Datele persoanelor vizate pot fi transferate in Israel si/sau in Cipru, tarile de apartenenta a asociatilor si investitorilor ce fac parte din grup.

Conform Deciziei Comisiei din 31.01.2011 in temeiul Directivei 95/46/CE a Parlamentului European si a Consiliului privind nivelul de protectie adecvat asigurat de Statul Israel privind prelucrarea automata a datelor cu caracter personal, se considera ca Statul Israel ofera un nivel adecvat de protectie a datelor cu caracter personal transferate din Uniunea Europeana in ceea ce priveste transferurile international automate de date cu caracter personal din Uniunea Europeana sau in cazul transferurilor neautomate, daca acestea sunt supuse unor prelucrari automate in Statul Israel.

In Cipru, prelucrarea datelor cu caracter personal se realizeaza in conformitate cu Legea. nr. 138 (I) 2001 privind prelucrarea datelor cu caracter personal, cu modificările ulterioare.

Pentru cazuri atipice, societatea va solicita Autoritatii Nationale de Supraveghere a Prelucrarii Datelor cu Caracter Personal permisiunea de a transmite datele personale in tari a caror legislatie nu prevede un nivel de protectie cel putin egal cu cel oferit de legea romana.

B. CERINTE SPECIFICE DE TRANSFER IN FUNCTIE DE TEMEIUL SI SCOPUL TRANSFERULUI

In absenta unei decizii a Comisiei care sa constate asigurarea unui nivel adecvat de protectie, datele cu caracter personal pot fi transferate catre state terte sau organizatii internationale doar daca:

(i) operatorul sau persoana imputernicita de operator a oferit garantii adecvate;
(ii) cu conditia sa existe drepturi opozabile si cai de atac eficiente pentru persoanele vizate.

Aceste garantii adecvate pot fi furnizate fara sa fie nevoie de nicio autorizatie specifica din partea unei autoritati de supraveghere, prin:

a) un instrument obligatoriu din punct de vedere juridic si executoriu intre autoritatile sau organismele publice;

b) reguli corporatiste obligatorii in conformitate cu articolul 47 din Regulament (in speta, reguli cu privire la transferul intre mai multe entitati parte ale aceluiasi grup);

c) clauze standard de protectie a datelor adoptate de Comisie in conformitate cu procedura de examinare mentionata la articolul 93 alineatul (2) din Regulament;

d) clauze standard de protectie a datelor adoptate de o autoritate de supraveghere si aprobate de Comisie in conformitate cu procedura de examinare mentionata la articolul 93 alineatul (2) din Regulament;

e) un cod de conduita aprobat in conformitate cu articolul 40 din Regulament, insotit de un angajament obligatoriu si executoriu din partea operatorului sau a persoanei imputernicite de operator din tara terta de a aplica garantii adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

f) un mecanism de certificare aprobat in conformitate cu articolul 42 din Regulament, insotit de un angajament obligatoriu si executoriu din partea operatorului sau a persoanei imputernicite de operator din tara terta de a aplica garantii adecvate, inclusiv cu privire la drepturile persoanelor vizate.

De mentionat ca Regulamentul limiteaza abilitatea operatorului sau persoanei imputernicite sa transfere date cu caracter personal in afara UE in cazul in care acest transfer are la baza doar analiza acestora cu privire la nivelul adecvat de protectie de care beneficiaza aceste date.

In absenta unei decizii a Comisiei privind caracterul adecvat al nivelului de protectie sau a unor garantii adecvate, un transfer de date cu caracter personal catre o tara terta sau o organizatie internationala poate avea loc numai in una dintre conditiile urmatoare:

a) persoana vizata si-a exprimat in mod explicit acordul cu privire la transferul propus, iar consimtamantul sau a fost unul informat;

b) transferul este necesar pentru executarea unui contract intre persoana vizata si operator sau pentru aplicarea unor masuri precontractuale adoptate la cererea persoanei vizate;

c) transferul este necesar pentru incheierea unui contract sau pentru executarea unui contract incheiat in interesul persoanei vizate intre operator si o alta persoana fizica sau juridica;

d) transferul este necesar din considerente importante de interes public;

e) transferul este necesar pentru stabilirea, exercitarea sau apararea unui drept in instanta;

f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci cand persoana vizata nu are capacitatea fizica sau juridica de a- si exprima acordul;

g) transferul se realizeaza dintr-un registru care, potrivit dreptului Uniunii sau al dreptului intern, are scopul de a furniza informatii publicului si care poate fi consultat fie de public in general, fie de orice persoana care poate face dovada unui interes legitim, dar numai in masura in care sunt indeplinite conditiile cu privire la consultare prevazute de dreptul Uniunii sau de dreptul intern in acel caz specific.

In cazul in care un transfer nu ar putea sa se intemeieze pe niciunul dintre temeiurile mentionate anterior, inclusiv dispozitii privind reguli corporatiste obligatorii, si nu este aplicabila niciuna dintre derogarile pentru situatii specifice, un transfer catre o tara terta sau o organizatie internationala poate avea loc numai in cazul in care:

a) transferul nu este repetitiv,

b) transferul se refera doar la un numar limitat de persoane vizate,

c) transferul este necesar in scopul realizarii intereselor legitime majore urmarite de operator asupra caruia nu prevaleaza interesele sau drepturile si libertatile persoanei vizate si

d) in urma unei evaluari a circumstantele aferente transferului de date, operatorul a prezentat garantii corespunzatoare in ceea ce priveste protectia datelor cu caracter personal.

In acest din urma caz, operatorul informeaza atat autoritatea de supraveghere cat si persoana vizata cu privire la transfer si la interesele legitime majore pe care le urmareste.

XI. MASURI TEHNICE SI ORGANIZATORICE

Pentru a asigura securitatea datelor personale prelucrate, societatea a adoptat urmatoarele masuri minime de siguranta:

- folosirea unui antivirus cu licenta;
- folosirea unui sistem de operare cu licenta;

- folosirea unui firewall;
- pseudonimizarea si criptarea datelor unde este cazul;
- acces restrictionat sau pe nivele la documentele fizice.

Pentru indeplinirea prevederilor legale aferente si in vederea satisfacerii cerintelor pastrarii in siguranta a datelor si informatiilor, societatea a elaborat si implementat masuri organizatorice si tehnice suplimentare, orientate pe anumite directii de actiune:

A. Identificarea si autentificarea utilizatorului

Prin utilizator se intelege orice persoana care actioneaza sub autoritatea operatorului, a persoanei imputernicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal.
Utilizatorii, pentru a primi acces la o baza de date cu caracter personal, trebuie sa se identifice. Identificarea se face prin introducerea codului de identificare de la tastatura (un sir de caractere).
Fiecare utilizator are propriul sau cod de identificare. Niciodata nu este alocat acelasi cod de identificare mai multor utilizatori.
Orice cont de utilizator este insotit de o modalitate de autentificare. Autentificarea se face prin introducerea unei parole.
Parolele sunt siruri de caractere, adecvate din punct de vedere al securitatii ca lungime si compozitie. La introducerea parolelor, acestea nu sunt afisate in clar pe monitor. Parolele sunt schimbate in mod periodic. Schimbarea periodica a parolelor se face numai de catre utilizatori autorizati de operator.
Orice utilizator care primeste un cod de identificare si un mijloc de autentificare este obligat prin fisa postului sa pastreze confidentialitatea acestora si sa raspunda in acest sens in fata operatorului.

B. Tipul de acces

Utilizatorii pot accesa numai datele cu caracter personal necesare pentru indeplinirea atributiilor de serviciu. Pentru aceasta sunt stabile tipurile de acces dupa functionalitate (administrare, introducere, prelucrare, salvare etc.) si dupa actiuni aplicate asupra datelor cu caracter personal (scriere, citire, stergere), precum si procedurile privind aceste tipuri de acces.

C. Colectarea datelor

Operatorul desemneaza utilizatori pentru operatiunile 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 utilizatorii desemnati de operator.
Operatorul a luat masuri pentru ca sistemul informational sa inregistreze cine a facut modificarea, data si ora modificarii.

D. Computerele si terminalele de acces

Toate calculatoarele, laptopurile, mijloacele electronice de stocare a informatiilor si a datelor personale şi alte terminale de acces sunt instalate in incaperi cu acces restrictionat si protejate prin parole cunoscute exclusiv de utilizatorul respectivului dispozitiv.
Serverele care gazduiesc bazele de date pot fi accesate doar in mod controlat, pe baza de drepturi de acces.
Nu este permisa scoaterea din companie a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD), decat cu aprobare prealabila din partea conducerii companiei.

E. Instruirea angajatilor

Operatorul face informarea personalului cu privire la prevederile GDPR, la cerintele minime de securitate pentru prelucrarile de date cu caracter personal, precum si cu privire la riscurile pe care le comporta prelucrarea datelor cu caracter personal, in functie de specificul activitatii.
Utilizatorii care au acces la date cu caracter personal sunt instruiti de catre operator asupra confidentialităţii acestora.
Utilizatorii au urmatoarele obligatii specifice:
a) sa cunoasca si sa aplice prevederile actelor normative din domeniul prelucrarii datelor cu caracter personal precum si ale prezentei proceduri;
b) sa informeze persoana vizata atunci cand datele cu caracter personal sunt colectate direct de la aceasta, in conditiile legii, cu privire la:
- identitatea si datele de contact ale operatorului;
- datele de contact ale responsabilului cu protectia datelor;
- scopul in care se face prelucrarea datelor cu caracter personal, precum si temeiul juridic al prelucrarii;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- perioada pentru care vor fi stocate datele cu caracter personal sau, daca acest lucru nu este posibil, criteriile utilizate pentru a stabili aceasta perioada;
- existenta dreptului de a solicita operatorului accesul la acestea, rectificarea sau stergerea acestora sau restrictionarea prelucrarii sau a dreptului de a se opune prelucrarii, precum si a dreptului la portabilitatea datelor;
- existenta dreptului de a retrage consimtamantul in orice moment, fara a afecta legalitatea prelucrarii efectuate pe baza consimtamantului inainte de retragerea acestuia;
- dreptul de a depune o plangere in fata unei autoritati de supraveghere;
- daca furnizarea de date cu caracter personal reprezinta o obligatie legala sau contractuala sau o obligatie necesara pentru incheierea unui contract;
- daca persoana vizata este obligata sa furnizeze aceste date cu caracter personal si care sunt eventualele consecinte ale nerespectarii acestei obligatii;
c) sa prelucreze numai datele cu caracter personal necesare indeplinirii atributiilor de serviciu si sa acorde sprijin conducatorului operatorului pentru realizarea activităţilor specifice ale acestuia;
d) sa pastreze confidentialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/ baze de date prin care sunt gestionate date cu caracter personal;
e) sa respecte masurile de securitate, precum si celelalte reguli stabilite de operator;

f) sa informeze de indata conducerea companiei despre imprejurari de natura a conduce la o diseminare neautorizata de date cu caracter personal sau despre o situatie in care au fost accesate/ prelucrate date cu caracter personal prin incalcarea normelor legale, despre care a luat la cunostinta.

In acest sens, se organizeaza saptamanal cate o sedinta de informare a angajatilor, prezenta acestora fiind obligatorie, iar periodic acestia sunt testati privind informatiile dobandite prin intermediul acestor sedinte.

F. Securizarea arhivei de documente

Toate documentele continand date cu caracter personal sunt depozitate in dulapuri prevazute cu incuietori la care are acces o singura persoana desemnata in acest sens responsabila cu accesul la documentatie.
Dulapurile sunt depozitate in camere prevazute cu incuietori, accesul fiind restrictionat.

G. Clauze speciale privind protectia datelor cu caracter personal in cuprinsul contractelor de prestari servicii

Se vor insera clauze speciale privind protectia datelor cu caracter personal in conformitate cu dispozitiile GDPR in toate contractele de prestari servicii ce vor fi incheiate de societate cu diversi contractori/furnizori/clienti.

XII. PROCEDURA PENTRU DEPUNERE CERERI/PLANGERI

Persoanele vizate se vor putea adresa cu o plangere impotriva modului de prelucrare a datelor, direct catre societate, in care vor arata solicitarea, motivul nemultumirii sau/si drepturile pe care le considera ca i-au fost incalcate si vor cuprinde mentiuni cu privire la optiunea de comunicare a raspunsului, respectiv pe suport fizic sau electronic.

Cererea, redactata in scris, va fi transmisa la sediul societatii sau pe email, la adresa datepersonale@mc-group.ro, persoana vizata urmand sa primeasca un raspuns in termen de 30 de zile de la data inregistrarii in evidentele societatii.
In cazul in care cererile din partea unei persoane vizate sunt in mod vadit nefondate sau excesive, in special din cauza caracterului lor repetitiv, societatea este indreptatita fie sa perceapa o taxa rezonabila tinand cont de costurile administrative pentru furnizarea informatiilor, fie va putea sa refuze sa dea curs solicitarii.

In afara de modalitatea mentionata mai sus de solutionare a eventualelor diferende, persoanele vizate au posibilitatea de a inainta (direct sau prin reprezentant) o plangere catre Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (www.dataprotection.ro).

Pentru orice intrebare despre modul in care datele persoanelor vizate sunt utilizate sau daca sunt necesare orice lamuriri suplimentare in legatura cu orice aspect ce tine de prelucrarea datelor, acestea se pot adresa responsabilului cu protectia datelor din cadrul companiei prin email la adresa datepersonale@mc-group.ro sau prin posta la adresa de sediu a societatii.

Prezenta Politica se completeaza cu dispozitiile Regulamentului intern de informare privind GDPR, cu posibilitatea revizuirii periodice, in functie de modificarile si completarile legislative aplicabile, precum si de nivelul de dezvoltare tehnologica si se completeaza cu prevederile legale privind prelucrarea datelor cu caracter personal si libera circulatie a acestor date.