ACORD PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL
La Contractul _____

Partile contractante:

Zipper Services S.R.L., organizata si functionand in conformitate cu legile din Romania, cu sediul social in Mun. Cluj - Napoca, str. Rene Jeannel, nr. 8, Imobil Novis Plaza, corp A, et. 2, jud. Cluj si adresa de corespondenta in Mun. Bucuresti, Bd. 1 Decembrie 1918, Nr. 1G, Sector 3, inmatriculata la Oficiul Registrului Comertului de pe langa Tribunalul Cluj sub nr. J2004003166129, Cod Unic de Inregistrare 16723187 - Atribut Fiscal RO, reprezentata de catre DORU IOAN VIJIIANU – Reprezentant al Administratorului DIV Total Consult SRL, in calitate de **Persoana Imputernicita de Operator**

Si

_____, avand sediul social in _____, inmatriculata la Oficiul Registrului Comertului de pe langa Tribunalul _____ sub nr. _____, Cod Unic de Inregistrare _____, reprezentata legal de catre _____ avand functia de _____, in calitate de **Operator;**

denumite in continuare in mod colectiv „**Partile**”, iar fiecare „**Parte**”.

- Avand in vedere adoptarea Regulamentului (UE) 2016/679 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”**, „**Regulamentul**” sau „**GDPR**”);

- Pe parcursul derularii Contractului, Operatorul va transfera catre Persoana Imputernicita de Operator date cu caracter personal care trebuie protejate conform legislatiei aplicabile:

- In conformitate cu prevederile Regulamentului general privind protectia datelor, prelucrarea de catre o persoana imputernicita de operatorul de date trebuie sa fie reglementata printr-un act juridic care sa aiba caracter obligatoriu pentru persoana imputernicita si subcontractorii acesteia in raport cu operatorul si care stabileste Obiectul, durata prelucrarii, natura si scopul, tipul de date cu caracter personal si categoriile de persoane vizate, obligatiile si drepturile operatorului;

1. Definitii

Termenii folositi cu majuscule in acest document au intelesul specificat in acest articol sau dupa cum este specificat in Acord. In masura in care prezentul Acord nu prevede altfel, restul termenilor si al expresiilor nedefiniti in prezentul Acord, incluzand, dar fara a se limita la, „date cu caracter personal” (in general), „prelucrare”, „autoritate de supraveghere”, „persoana vizata”, „reprezentant”, „organizatie internationala”, au semnificatia prevazuta in GDPR.

a. „**Date cu caracter personal**“ inseamna orice informatii privind o persoana fizica identificata sau identificabila („Persoana Vizata”); o persoana 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.

b. „**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.

c. „**Prelucrare**" inseamna orice operatiune sau set de operatiuni efectuate asupra Datelor cu caracter personal, incluzand fara limitare colectarea, inregistrarea, pastrarea, modificarea, utilizarea, dezvaluirea, accesul, transferul sau distrugerea acestora.

d. „**ANSPDCP**" inseamna Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu caracter personal din Romania sau, dupa caz, autoritatea competenta pentru protectia datelor din cadrul Uniunii Europene.

e. **„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;

f. **„Contractul"** contractul nr. _____, incheiat de catre Parti, avand ca obiect _____ ;

g. **„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;

h. **„Persoana Imputernicita de operator"** inseamna persoana fizica sau juridica, autoritatea publica, agentia sau alt organism care prelucreaza datele cu caracter personal in numele operatorului;

i. **Subcontractor,** inseamna persoana fizica sau juridica, care prelucreaza datele cu caracter personal in numele Persoanei Imputernicita de Operator sau al unui Subcontractor al Persoanei Imputernicite;

j. **„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;

k. **„parte terta**" inseamna o persoana fizica sau juridica, autoritate publica, agentie sau organism altul decat persoana vizata, 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;

l. **„sistem de evidenta a datelor"** inseamna orice set structurat de date cu caracter personal accesibile conform unor criterii specifice fie ele centralizate, descentralizate sau repartizate dupa criteriile functionale sau geografice;

m. **„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 Regulament, care reprezinta operatorul sau persoana imputernicita in ceea ce priveste obligatiile lor respective care le revin in temeiul prezentului regulament;

n. **„restrictionarea prelucrarii"** inseamna marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

2. Obiectul si durata prelucrarii

Obiectul prezentului Acord il reprezinta prelucrarea datelor cu caracter personal necesare indeplinirii obiectului Contractului.

Operatorul este unicul proprietar al Datelor cu caracter personal furnizate Persoanei imputernicite, astfel incat Operatorul are dreptul de a stabili modul de Prelucrare a Datelor cu caracter personal de catre Persoana Imputerncita.

Persoana imputernicita de operator se va conforma tuturor legilor aplicabile referitoare la furnizarea serviciilor in baza Contractului, incluzand fara a se limita la toate legile aplicabile referitoare la confidentialitatea si securitatea Datelor cu caracter personal Prelucrate de catre Persoana imputernicita de Operator pentru si in numele Operator.

In cazul in care oricare Parte va divulga celeilalte Parti date cu caracter personal privind angajații sau reprezentanții sai responsabili cu executarea prezentului contract, acestea vor consta in: nume, prenume, functia, numar de telefon, adresa de email a angajatilor/reprezentantilor relevanti.

Fiecare Parte care divulga informatii in legatura cu angajatii/reprezentantii sai trebuie sa furnizeze o nota de informare persoanelor vizate, informandu-le in mod corespunzator cu privire la prelucrarea datelor cu caracter personal ale acestora, efectuata de catre cealalta Parte in legatura cu prezentul contract, aceasta avand obligatia de a actiona doar in baza Instructiunilor primite de la celalata parte si de a aplica masurile tehnice si organizatorice adecvate pentru protejarea Datelor cu caracter personal impotriva distrugerii accidentale sau ilegale, pierderii, modificarii, dezvaluirii sau accesului neautorizat, in special daca prelucrarea respectiva comporta transmitere de date in cadrul unei retele, precum si impotriva oricarei alte forme de prelucrare ilegala.

Masurile tehnice si organizatorice considerate a fi adecvate de catre parti sunt cele indicate in Anexa 1 - Masuri tehnice si organizatorice, parte integranta a prezentului acord.

Durata prelucrarii nu poate fi mai mare decat durata contractului mai sus mentionat, cu exceptia situatiei in care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal.

Persoana imputernicita de operator nu poate schimba scopurile si utilizarile datelor si nici nu poate folosi datele in scopuri proprii, fiind strict interzise comunicarile in scop de marketing, transferul datelor in strainatate, precum si orice prelucrare de date cu caracter personal care exced indeplinirii obiectului contractului mai sus mentionat.

Natura datelor cu caracter personal: .....

Obiectul si scopul prelucrarii datelor cu caracter personal de catre Persoana Imputernicita pentru Operator sunt clar definite in cadrul contractului de prestari servicii mai sus mentionat

Tipul de date cu caracter personal prelucrate: .....

Categoriile de persoane vizate: .....

Operatiuni de prelucrare a datelor cu caracter personal, din perspectiva Persoanei Imputernicite de Operator, care au loc pentru indeplinirea serviciilor:

Tip	DA/NU	Tip	DA/NU	Tip	DA/NU
colectare	DA	modificare	DA	aliniere	DA
inregistrare	DA	extragere	DA	combinare	DA
organizare	DA	consultare	DA	restrictionarea	NU
structurare	DA	utilizare	DA	stergerea	DA
stocare	DA	divulgare prin transmitere	DA	distrugerea	DA
adaptare	NU	diseminare	DA	Altele	NU

3. Instructiunile Operatorului

Persoana imputernicita de operator declara ca a luat la cunostinta ca operatorul are dreptul de a transmite Instructiuni privind prelucrarea datelor cu caracter personal, ce devin parte integranta din contract si care isi produc efectele de la data comunicarii acestora, urmand ca in caz de conflict intre prevederile din contract, celelalte anexe si Instructiunile comunicate de catre Operator in aplicarea Regulamentului (UE) 2016/679 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-RGPD) sa prevaleze Instructiunile.

4. Obligatiile Imputernicitului

Persoana imputernicita de operator:

a) va pune in aplicare masuri tehnice si organizatorice adecvate, asa cum acestea sunt redate in **Anexa 1 - Masurile tehnice si organizatorice**, astfel incat prelucrarea sa respecte cerintele prevazute in cadrul Regulamentului si sa asigure protectia drepturilor persoanei vizate (dreptul la informare, dreptul de acces, dreptul la rectificare, dreptul la stergerea datelor, dreptul la restrictionarea prelucrarii, dreptul la portabilitatea datelor, dreptul la opozitie si procesul decizional individual automatizat);

b) persoanele autorizate sa prelucreze datele cu caracter personal au o obligatie contractuala/statutara adecvata de confidentialitate si prelucreaza aceste date numai in exercitarea atributiilor contractuale/statutare;

c) va asista operatorul prin masuri tehnice si organizatorice adecvate, in masura in care acest lucru este posibil, pentru indeplinirea obligatiei operatorului de a raspunde cererilor privind exercitarea de catre persoana vizata a drepturilor prevazute de Regulament; va pune la dispozitia Operatorului toate informatiile necesare si pe care le detine pentru a demonstra respectarea obligatiilor ce ii revin;

d) va permite, va contribui si va asigura suportul necesar pentru desfasurarea auditurilor, inclusiv a inspectiilor, efectuate de operator sau alt auditor mandatat de operator, cu indeplinirea cumulativa a urmatoarelor conditii:

- Operatorul va transmite Persoanei imputernicite o notificare scrisa cu cel putin 15 (cincisprezece) zile lucratoare inainte de data inceperii auditului;

- auditul se va desfasura in timpul programului normal de lucru al Persoanei Imputernicite;

- orice document solicitat in scopul auditului de catre Operator sau mandatarul acestuia va fi in directa legatura de cauzalitate cu prelucrarea datelor cu caracter personal;

- scopul auditului va viza exclusiv modul de executare a Contractului, respectiv indeplinirea obligatiilor de catre Persoana imputernicita cu privire la prelucrarea datelor cu caracter personal. va coopera cu autoritatea de supraveghere;

e) va prelucra date cu caracter personal numai la cererea Operatorului, pe baza instructiunilor acestuia si in limitele stabilite prin contract cu respectarea legislatiei privind prelucrarea datelor personale la care are acces, indiferent in ce forma, cu exceptia cazului in care legislatia UE sau legislatia nationala il obliga sa faca acest lucru;

f) va asigura, anterior prelucrarii, instruirea privind protectia prelucrarii Datelor cu caracter personal tuturor persoanelor care au acces la acestea;

g) Persoana imputernicita de operator va raspunde, pentru orice prejudiciu suferit de catre operator/persoana vizata, in caz de nerespectare a obligatiilor ce rezulta din legislatia privind protectia datelor cu caracter personal care revin mod specific persoanelor imputernicite de operator, precum si pentru nerespectarea instructiunilor operatorului puse la dispozitia sa de catre acesta. In cazul in care Instructiunile puse la dispozitia Persoanei Imputernicite nu sunt legale sau in neconcordanta cu prevederile RGDP si conduc la un prejudiciu material sau moral provocat persoanei vizate, ca urmare a unei incalcari a regulamentului RGDP, Persoana imputernicita de operator este exonerata de raspundere daca dovedeste ca nu este raspunzatoare in niciun fel pentru evenimentul care a cauzat prejudiciul.

La solicitarea operatorului/autoritatilor competente persoana imputernicita de operator va prezenta dovezi rezonabile privind respectarea instructiunilor operatorului.

5. Obligatiile Operatorului

a) Operatorul se va asigura ca are o politica de confidentialitate si ca persoanele vizate au fost informate cu privire la transferul Datelor lor cu caracter personal catre Persoana imputernicita pentru durata, scopul, categoriile si tipurile de date cu caracter personal stabilite in actele incheiate intre Parti, respectiv, dar fara a ne limita la, prezentul document ce contine Instructiuni privind prelucrarea datelor cu caracter personal.

b) Operatorul va informa Împuternicitul, fara întârzieri nejustificate și în mod cuprinzator, asupra oricaror nereguli sau greșeli pe care acesta le va detecta în activitatea de prelucrare desfașurata de Operator sau în ceea ce privește implementarea cerințelor legale privind protecția datelor.

c) Operatorul declara si garanteaza ca Prelucrarea Datelor cu caracter personal a fost efectuata cu respectarea dispozitiilor legale in materie si isi asuma intreaga raspundere pentru colectarea si transferarea acestor Date Persoanei Imputernicite cat si pentru Instructiunile date Persoanei Imputernicite in acest sens.

6. Dezvaluirea neautorizata de date cu caracter personal

Persoana imputernicita de operator are obligatia de a informa Operatorul (la datele de contact mentionate la pct. 6) de indata, ce ia la cunostinta, dar nu mai tarziu de 72 ore, cu privire la toate situatiile de constatare a unei incalcari a securitatii datelor cu caracter personal, in vederea luarii masurilor de remediere si/sau sesizarii organelor competente, dupa caz.

Toate instructiunile comunicate de catre Operator in aceste situatii vor fi respectate de indata de catre Persoana imputernicita de operator pentru limitarea la minimum a posibilelor diseminari si/sau pagube.

Informarea care se transmite operatorului va contine urmatoarele informatii, daca sunt disponibile si numai in masura in care Persoana imputernicita le detine:

a) descrierea incalcarii securitatii datelor cu caracter personal;
b) numele si datele de contact ale responsabilului cu protectia datelor sau unui alt punct de contact pentru a obtine mai multe informatii (daca s-au modificat);
c) descrierea posibilelor consecinte ale incalcarii securitatii datelor cu caracter personal;
d) descrierea masurilor adoptate sau propuse pentru remedierea problemei incalcarii securitatii datelor cu caracter personal, inclusiv, daca este cazul, masurile adoptate pentru a atenua posibilele negative efecte.

In situatia in care informatiile nu pot fi furnizate simultan si in masura in care acestea nu sunt disponibile de indata, acestea vor fi furnizate treptat, fara intarzieri nejustificate.

7. Responsabili cu protectia datelor

Din partea OPERATORULUI	**Din partea PERSOANEI IMPUTERNICITE DE OPERATOR**
Nume, prenume: _____	Nume, prenume: Mirela Ojog
e-mail: _____	e-mail: dpo@ezipper.ro; mirela.ojog@ezipper.ro
fax: _____	fax: 0213404636
tel: _____	tel: 0213404638
adresa de corespondenta _____	adresa de corespondenta: Bd. 1 Decembrie 1918, nr 1G, Sector 3 Bucuresti

8. Subcontractarea

Persoana imputernicita de operator nu poate subcontracta drepturile si obligatiile din prezentul contract fara acordul scris prealabil al Operatorului, specific sau general. In cazul unei autorizatii generale scrise, persoana imputernicita de operator informeaza operatorul cu privire la orice modificari preconizate privind adaugarea sau inlocuirea altor persoane imputernicite de operator, oferind astfel posibilitatea operatorului de a formula obiectii fata de aceste modificari.

Operatorul este de acord ca Persoana Imputernicita sa recruteze o alta persoana imputernicita (denumita in continuare „Parte Terta") in vederea prelucrarii Datelor cu Caracter Personal in baza acestui contract. Persoana imputernicita garanteaza ca a semnat sau semneaza un contract scris cu Partea Terta care sa incorporeze obligatii privind protectia datelor care sa ofere suficiente garantii ca dispozitiile GDPR sunt respectate in totalitate. Persoana imputernicita ramane pe deplin raspunzatoare fata de Operator in ceea ce priveste indeplinirea obligatiilor Partii Terte in legatura cu acest contract.

La solicitarea Operatorului, Persoana Imputernicita ofera informatii privind Partea Terta, activitatea desfasurata precum si orice alte informatii considerate necesare de catre Operator si care au legatura cu prelucrarea datelor cu caracter personal de catre Partea Terta. Operatorul poate solicita Persoanei Imputernicite, in baza unor motive temeinice, incetarea contractului cu Partea Terta.

Constituie exeptie de la dispozitiile prezentului articol serviciile de distributie postala, realizate prin furnizori specializati si aprobati in prealabil de catre Operator:

Nr. crt.	Societate subcontractoare/ Parte Terta	Adresa/tara	Serviciul subcontractat
1.			
2.			

9. Confidentialitate

Partile se obliga sa pastreze confidentialitatea datelor, informatiilor si documentelor pe care le vor detine ca urmare a executarii Contractului .

Persoana imputernicita nu va dezvalui Datele cu caracter personal Prelucrate pentru si in numele Operatorului niciunei persoane sau entitati, fara aprobarea scrisa prealabila din partea acestuia, cu exceptia cazurilor in care:

- acest lucru este necesar pentru prestarea serviciilor corespunzatoare Contractului;
- o asemenea dezvaluire este ceruta prin legile aplicabile sau proceduri legale obligatorii, caz in care Persoana imputernicita va:
    - notifica imediat, in scris, Operatorul, inainte de a raspunde unei asemenea cereri de dezvaluire;
    - va face tot posibilul pentru a limita natura si scopul respectivei dezvaluiri;
    - va dezvalui un volum minim de Date cu caracter personal necesare pentru a se conforma legilor aplicabile sau solicitarilor/ ordinelor legale; si
    - va urma toate instructiunile rezonabile ale Operatorului referitoare la asemenea dezvaluiri.

10. Incetarea prelucrarii

In termen de 90 de zile de la finalizarea serviciilor de prelucrare a datelor cu caracter personal corespunzatoare Contractului, acest lucru insemand predarea catre furnizorul de servicii postale, sau mai devreme, la cererea Operatorului formulata in scris, Persoana Imputernicita va returna, daca Operatorul solicita acest lucru in termenul specificat mai sus, sau va sterge toate documentele si seturile de date referitoare la Contract si care au intrat in posesia sa, cu exceptia situatiei in care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal. Acelasi lucru este valabil pentru toate materialele legate de testare sau deseuri redundante.

Daca Operatorul solicita in scris in termen de 1 an de la finalizarea serviciilor de prelucrare, Persoana Imputernicita va confirma, prin intermediul unei notificari scrise pe care o va transmite Operatorului, faptul ca au fost indeplinite operatiunile de returnare, stergere sau distrugere conform dispozitiilor acordului.
Niciun fel de reclamatie/sesizare nu va fi luata in considerare de catre Persoana Imputernicita, daca a fost formulata de catre Operator, fata de activitatile realizate de Persoana Imputernicita in cadrul Contractului, dupa expirarea termenului de stergere prevazut mai sus, partiile fiind de acord ca acesta reprezinta un termen de decadere din dreptul de depune astfel de reclamatii.

Stergerea reprezinta o actiune care determina in mod ireversibil ca o informatie sau o data ce se refera la o persoana, sa nu poata fi extrasa din datele stocate. Va face obiectul stergerii, respectiv distrugerii orice prelucrare si utilizare a rezultatelor prelucrarii.

11. Prevederi finale

Orice modificari aduse prezentului Acord trebuie facute în scris, putând fi efectuate numai printr-un act adițional scris semnat de ambele parți.

În cazul în care una sau mai multe prevederi mai sus menționate este sau devine nula sau incompleta, parțial sau în întregime, nu va afecta validitatea celorlalte prevederi.

Orice litigii sau revendicari aparute în temeiul Acordului, inclusiv litigiile privind existența, validitatea sau încetarea acestuia se supun jurisdicției alese prin Contractul Cadru.

Prevederile prezentului Acord in ceea ce priveste prelucrarea datelor cu caracter personal au prioritate fata de orice alte intelegeri, sau conventii (scrise sau verbale) anterioare incheiate intre parti si care reglementeaza acest aspect.

Prezentul Acord a fost incheiat astazi, _____, in 2 (doua) exemplare originale, cate unul pentru fiecare parte contractanta, si intra in vigoare la data semnarii de catre ambele parti.

OPERATOR

PERSOANA IMPUTERNICITA DE OPERATOR

S.C. ZIPPER SERVICES S.R.L.

DORU IOAN VIJIIANU – Reprezentant al Administratorului DIV Total Consult SRL

Anexa 1 - Masuri tehnice si organizatorice la
ACORD PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL
La Contractul _____

Descrierea generală a măsurilor de securitate tehnice și organizatorice menționate la Articolul 32 alineatul (1) din RGPD:

1.Condiții privind Confidențialitatea (Articolul 32 Alineatul 1 Punctul b din Regulament)

1.1 Controlul accesului fizic

(1) Clădirile sunt protejate printr-un sistem de supraveghere video și alarme de pătrundere nelegală;
(2) Accesul fizic în clădiri se realizeaza pe bază de card acces si este consemnat nominal
(3) Zonele in care sunt procesate date cu caracter personal sunt prevazute cu senzori de efractie si senzori de incendiu; Exista contract cu firma de interventie in caz de efractie si incendiu;
(4) Regulile şi normele de lucru şi acces în zonele de securitate sunt definite şi aplicate, iar drepturile de acces la zonele de securitate sunt revizuite şi reînnoite în mod regulat.

1.2 Controlul electronic al accesului

(1) Rețeaua companiei este protejată de rețeaua publică prin firewall
(2) Angajații sunt obligați să respecte un regulament cu următoarele specificații:
- ✓ parole individuale secrete
- ✓ lungime minima a parolei si norme de complexitate a parolei (litera mare, litera mica, cifra si caracter special)
- ✓ modificarea parolei la intervale regulate de timp
- ✓ aplicarea unei politici de tipul „birou curat, ecran protejat” in scopul evitării păstrării documentelor pe biroul de lucru şi lăsării staţiilor de lucru neprotejate

(3) Obligaţiunile funcţionale (rolurile) şi domeniile de responsabilitate sunt adecvat segregate, pentru a reduce posibilităţile de utilizare abuzivă a resurselor informaţionale ale entităţii (de ex. segregarea funcţiilor de administrare a bazelor de date, a sistemelor de operare, a serviciilor de reţea, respective a functiilor de elaborare si testare a sistemelor informatice).
(4) Există proceduri şi măsuri de securitate care să permită accesul la sistemele de operare pe staţiile utilizatorilor şi pe servere doar pentru utilizatorii autorizaţi (administrator).
(5) Soluţiile antivirus se actualizează periodic, rulează permanent şi nu pot fi stopate neautorizat. Software-ul antivirus este folosit:
- in toate canalele de comunicatie cu rețeaua companiei: Internet, Email, fisiere (ex. pe FTP)
- pentru toate serverele si toate unitățile individuale de muncă/laptopuri
(6) Patch-uri relevante pentru siguranța software-ului sunt instalate automat si la intervale regulate de timp
(7) Drepturile de acces sunt acordate (diferentiat in functie de obligatiumile functionale) in baza unui formular de acordare drepturi, in conformitate cu procedurile interne existente;
(8) Se realizeaza scanarea periodica a vulnerabilitatilor (atat intern prin tooluri adecvate, cat si extern prin firma externa specializata in acest sens) in conformitate cu procedurile interne existente.
(9) Verificările de pătrundere a adreselor IP expuse pe Internet sunt realizate la intervale regulate de timp (penetration test)
(10) Toţi angajaţii se instruiesc pentru a raporta orice vulnerabilitate de securitate observată sau suspectată în cadrul sistemelor sau a serviciilor.

2. Integritatea (Articolul 32 Alineatul 1 Punctul b din Regulament)

2.1 Controlul transferului de date

(1) Schimbul de informaţii dintre Client si Furnizor (Operator si Persoana imputernicita de operator) se efectuează în baza unui acord semnat (contract), ce să includă mijloacele, cerinţele şi responsabilităţile aferente securităţii informaţiei.
(2) Se pot aplica diferite protocoale de securizare a comunicatiilor (pe nivelul legaturii de date, de retea, de transport, de aplicatie) precum: protocoale de tunelare (IPSec/SSL VPN), sFTP, FTPs, HTTPS, care se vor stabili in acordul semnat.

2.2 Controlul introducerii datelor

(1) Controlul transferului de date dintre Client si Furnizor este asigurat prin canale securizate de transfer, conform 2.1.

(2) Datele trimise prin suporturi de date (i.e. stick USB, HDD extern) sunt criptate si se utilizeaza doar ca solutie de back-up pentru transferul de date in situatia existentei unui blocaj de transfer electronic

(3) Fisierele ce contin date cu caracter personal sunt criptate la un interval de timp de la procesare (date at-rest) in conformitate cu specificatiile contractuale.

(4) Datele clienților sunt șterse la un interval de timp de la procesare, in conformitate cu prevederile contractuale

3.Pseudonimizarea (Articolul 32 Alineatul 1 Punctul a din Regulament; Articolul 25 Alineatul 1 din Regulament)

(1) Pseudonimizarea doar a bazelor de date ce vor fi stocate de persoana imputernicita de operator la solicitarea expresa a operatorului dupa finalizarea furnizarii serviciilor legate de prelucrare

4.Disponibilitatea și rezistența sistemelor (Articolul 32 Alineatul 1 Punctul b din Regulament)

(1) Este stabilită o politică de efectuare a copiilor de rezervă ce să asigure efectuarea regulată a copiilor de rezervă şi păstrarea lor în condiţii de siguranţă. Politica de efectuare a copiilor de rezervă stabileste tipul datelor, frecvenţa efectuării copiilor de rezervă şi modalitatea de păstrare a lor, ţinând cont de importanţa informaţiei, cerinţele actelor normative în vigoare şi rezultatele analizei de risc.

(2) Copiile de rezervă se păstrează în condiţii ce să asigure integritatea şi disponibilitatea lor în caz de necessitate.

(3) Prevenirea distrugerii sau pierderii accidentale sau intenționate a datelor este asigurata si prin:

- ✓ alimentare neîntreruptibilă (UPS),
- ✓ protecția antivirus,
- ✓ firewall,
- ✓ proceduri de raportare incidente de securitate
- ✓ planuri pentru situații de urgență

5. Recuperarea rapidă si Control al Accesibilitatii (Articolul 32 Alineatul 1 Punctul c din Regulament)

(1) Pentru reproducerea ștergerii sau modificarea datelor clientului, fișierele de înregistrare personale sunt activate pe sistemele relevante IT:

(2) Există un concept de acces restrâns pentru prevenirea modificării fișierelor de înregistrare personale menționate sus

(3) Locul de stocare a suporturilor de date a copiilor de rezervă se afla la o distanta > 3 KM

(4) Există acorduri de mentenanță privind mentenanța sistemelor IT de către terți.

6. Control al Conformării

(1) Măsuri de implementare comprehensive a metodologiei de protecție a datelor sau informațiilor de siguranță:

- ✓ ISO 27001,
- ✓ ISO 20000-1,
- ✓ centru de date acreditat MCSI
- ✓ administrator de arhiva electronica autorizat MCSI.

7.Proceduri de testare, verificare și evaluare regulată (Articolul 32 Alineatul 1 Punctul d din Regulament; Articolul 25 Alineatul 1 din Regulament)

7.1. Managementul protecției datelor si Control al Muncii

(1) Se pot obtine declarații adiționale scrise (în legătură cu protecția datelor și siguranța datelor):

- ✓ la cerere prin Acord de Confidențialitate
- ✓ în general printr-o clauză obișnuită de confidențialitate inclusă în contractul de muncă

(2) Subcontractanții care au acces la datele clientului sunt/au fost autorizați

(3) Există măsuri de instruire a angajaților cu privire la Siguranța Informațiilor în general și Actul de Protecția Datelor în particular.

7.2. Controlul Contractului se va efectua:

(1) în baza dispozițiilor Regulamentului privind protecția datelor cu caracter personal, astfel încât nicio procesare a datelor de către terți, în conformitate cu Articolul 28 GDPR, să nu fie făcută în absența unor instrucțiuni ale Clientului în acest sens
(2) Externalizarea necesită acordul expres al Beneficiarului (exprimat în prealabil, în scris);
(3) Exista masuri de instruire a angajatilor cu privire la Siguranta informatiilor in general si actul de protectia datelor cu caracter general

7.3 Managementul răspunsului la incidente (art. 24)

(1) Responsabilităţile şi procedurile de reacţiune la incidentele de securitate sunt explicit stabilite în cadrul poloiticilor de securitate, pentru a asigura un răspuns rapid, eficient şi sistematic la incidentele de securitate a informaţiei.
(2) Probele aferente incidentelor de securitate se colectează şi păstrează în condiţii de siguranţă în scopul investigării incidentelor şi asigurării suportului în cazul eventualelor acţiuni legale legate de incidentele petrecute. Se asigură înregistrarea, documentarea completă şi raportarea incidentelor de securitate.
(3) Exista politici adecvate de protecție a datelor cu caracter personal
(4) Exista coduri de conduită /proceduri specifice sectorului de activitate și de nevoile companiei în care se reflectă principiile art. 40 din Regulament

8. Proceduri de verificare a existentei persoanei responsabile conform art.7 din Regulamentul 679/2016

(1) Beneficiarul / Operatorul a desemnat, conform art. 37 din Regulamentul 679 / 2016, un responsabil cu protecția datelor:
(2) Persoana imputernicita a desemnat, conform art. 37 din Regulamentul 679 / 2016, un responsabil cu protecția datelor:

9. Masuri organizatorice generale

(1) Exista politici de securitate a informatiei (ex. control acces, managementul parolelor, utilizare email, utilizare internet, back-up, accesul la distanta, utilizarea dispozitivelor mobile, tratarea incidentelor, etc.)
(4) Exista implementat si testat anual un Plan de continuitate al afacerii
(5) Evaluarea riscurilor de securitate a informatiei
(6) Angajatii au semnat acord de confidentialitate
(7) Distrugerea documentelor se face direct de catre companie prin tocatoarele proprii care indeplinesc cerintele legate de securitate sau de catre firme specializate in distrugere securizata de documente;

OPERATOR

PERSOANA IMPUTERNICITA DE OPERATOR

S.C. ZIPPER SERVICES S.R.L.

DORU IOAN VIJIIANU – Reprezentant al Administratorului DIV Total Consult SRL