ACORD GENERAL PRIVIND PRELUCRAREA DATELOR

Articolul 28 din Regulamentul UE 2016/679 („**RGPD**”)

Între

Clientul, astfel cum este identificat în Contract („Operatorul”), reprezentat de reprezentantul său legal cu puterile necesare, în calitate de

Operator de date

și

Furnizorul, astfel cum este identificat în Oferta Comercială și în Anexa A la Condițiile Generale, reprezentat de reprezentantul său legal învestit cu puterile necesare („**Împuternicitul”** sau „**Furnizorul**”), în calitate de

Persoană împuternicită de operator

De asemenea, Operatorul și Împuternicitul pot fi denumiți împreună „**Părțile”** și individual „**Partea”**.

AVÂND ÎN VEDERE CĂ

I. Părțile au încheiat unul sau mai multe contracte („**Contractul”**) pentru furnizarea de Servicii („**Serviciile”**);
II. Contractul implică prelucrarea unor informații definite de lege ca Date cu Caracter Personal, iar Părțile intenționează, prin urmare, să reglementeze, în cadrul prezentului Acord General privind Prelucrarea Datelor („**Acordul**”), termenii și condițiile prelucrării Datelor cu Caracter Personal efectuate de Împuternicit în contextul furnizării Serviciilor în temeiul Contractului;
III. Detaliile și caracteristicile specifice sau condițiile particulare ale prelucrării Datelor cu Caracter Personal sunt cuprinse în așa-numitele „**Fișe de Prelucrare**” referitoare la unul sau mai multe Servicii activate de Client, care vor fi anexate la prezentul Acord la momentul relevant.
IV. Aceste Fișe de Prelucrare vor detalia metodele operaționale de prelucrare în raport cu Serviciul specific, indicând, după caz, lista Subîmputerniciților și orice măsuri de securitate suplimentare aplicate. Fișele de Prelucrare, odată semnate, vor fi incluse ca Anexe suplimentare la prezentul Acord și vor face parte integrantă și substanțială din acesta;
V. Înainte de a încredința Împuternicitului prestarea Serviciilor, Operatorul a verificat experiența, capacitatea și fiabilitatea Împuternicitului și a evaluat că acesta oferă garanții suficiente pentru implementarea unor măsuri tehnice și organizatorice adecvate și pentru asigurarea unei protecții adecvate a datelor prelucrate și a drepturilor persoanelor vizate;
VI. Împuternicitul trebuie să efectueze operațiunile de Prelucrare în conformitate cu instrucțiunile furnizate în scris de Operator printr-un contract sau alt act juridic obligatoriu care specifică durata, natura și scopurile Prelucrării, categoriile de Date cu Caracter Personal prelucrate și categoriile de persoane vizate implicate în Prelucrare, precum și obligațiile și drepturile Împuternicitului cu privire la Prelucrare;
VII. Prin prezentul Acord, Operatorul intenționează să desemneze Împuternicitul indicat în preambul ca persoană împuternicită de operator și să furnizeze toate instrucțiunile necesare pentru Prelucrarea Datelor cu Caracter Personal aferente furnizării Serviciilor;
VIII. Operatorul autorizează Împuternicitul, precum și persoanele autorizate de acesta, să acceseze numai Datele cu Caracter Personal strict necesare pentru executarea Contractului („**Datele cu Caracter Personal”**);
IX. Prezentul Acord nu implică niciun drept al Împuternicitului la tarife și/sau indemnizații și/sau rambursări specifice, altele decât cele eventual prevăzute deja în Contract, cu excepția implementărilor suplimentare solicitate în mod specific și convenite între Părți printr-un acord scris separat;
X. Furnizarea efectivă a Serviciilor care fac obiectul Contractului poate fi realizată, pentru fiecare Serviciu, de o anumită societate din Grupul Namirial, identificată în Fișele de Prelucrare relevante ca „Entitate Prestatoare”. Atunci când Entitatea Prestatoare nu coincide cu Împuternicitul, aceasta va opera în temeiul unor acorduri intra-grup între societățile Grupului Namirial, conforme cu articolul 28 din RGPD, preexistente și separate de prezentul Acord, fără a aduce atingere oricărui rol diferit în materie de protecție a datelor specificat în mod expres în Fișa de Prelucrare relevantă;
XI. În cazul în care Clientul acționează în calitate de persoană împuternicită în numele unui alt operator („Clientul Final”), Clientul însuși își va asuma, în legătură cu respectiva prelucrare

specifică, obligațiile și responsabilitățile unei persoane împuternicite față de Furnizor, care în acest context va prelua rolul de Subîmputernicit. Într-o astfel de situație, se vor aplica dispozițiile referitoare la prelucrarea datelor și obligațiile Împuternicitului în temeiul prezentului Acord, dar cu Clientul acționând în calitate de Împuternicit în numele Clientului Final și cu Împuternicitul acționând în calitate de Subîmputernicit în numele Clientului;

XII. În orice caz în care Clientul acționează în calitate de Operator sau de Împuternicit în numele Clientului Final, Împuternicitul este de acord să acționeze în calitate de Împuternicit și/sau Subîmputernicit și, prin urmare, se angajează să prelucreze Datele cu Caracter Personal în conformitate cu instrucțiunile primite de la Client și într-un mod care să asigure protecția Datelor cu Caracter Personal, potrivit măsurilor de securitate stabilite în prezentul Acord și în Fișele de Prelucrare anexate acestuia.

PRIN URMARE, PĂRȚILE CONVIN ȘI STIPULEAZĂ URMĂTOARELE

1. VALIDITATEA PREAMBULULUI ȘI A ANEXELOR. DEFINIȚII

1.1. Preambulul și Anexele fac parte integrantă și substanțială din prezentul Acord.

1.2. Cu excepția cazului în care se prevede altfel în prezentul Acord, toți termenii cu majuscule utilizați în prezentul Acord și în Anexe vor avea semnificația atribuită acestora în Contract și se vor înțelege ca fiind exprimați atât la singular, cât și la plural. În conformitate cu definițiile cuprinse în legislația aplicabilă, se utilizează termenii și definițiile prevăzute în **Anexa I – Definiții** la prezentul Acord, la care se face trimitere.

1.3. Fișele de Prelucrare referitoare la Serviciile utilizate de Client pot deveni parte a prezentului Acord, chiar și ulterior, în cazul completării Contractului pentru activarea de noi Servicii. În acest caz, Anexele, semnate de Părți împreună cu addendumul contractual, vor fi încorporate în prezentul Acord.

2. DREPTURILE ȘI OBLIGAȚIILE OPERATORULUI

2.1. Operatorul încredințează Împuternicitului toate – și exclusiv – operațiunile de Prelucrare a Datelor cu Caracter Personal necesare pentru executarea integrală a Contractului.

2.2. Operatorul declară că respectă toate obligațiile prevăzute de Legislația Aplicabilă în sfera sa de competență în legătură cu Prelucrarea Datelor cu Caracter Personal în temeiul prezentului Acord. În special, Operatorul:

a. are dreptul și obligația de a lua decizii cu privire la scopurile și mijloacele Prelucrării, inclusiv identificarea temeiului juridic corect al Prelucrării;
b. declară că Datele cu Caracter Personal sunt relevante și neexcesive în raport cu scopurile pentru care au fost colectate și prelucrate ulterior și sunt transmise cu respectarea tuturor cerințelor prevăzute de Legislația Aplicabilă;
c. întocmește și – acolo unde este necesar – pune la dispoziția Împuternicitului informații adecvate și complete privind Prelucrarea Datelor cu Caracter Personal în conformitate cu art. 13 și/sau art. 14 din RGPD.

2.3. Operatorul se angajează să notifice oficial Împuternicitului orice modificări care ar putea fi necesare cu privire la operațiunile de Prelucrare a Datelor cu Caracter Personal. Împuternicitul și Persoanele sale Autorizate nu vor efectua operațiuni de Prelucrare a Datelor cu Caracter Personal altele decât cele indicate de Operator în conformitate cu prezentul articol.

2.4. Operatorul garantează că infrastructurile și sistemele eventual puse la dispoziție de Operator și/sau de terți desemnați de acesta, pe care Împuternicitul va fi chemat să efectueze Prelucrarea („Sistemele Operatorului”), sunt adecvate, respectă standardele de referință și reglementările sectoriale și sunt în măsură să asigure furnizarea regulată a Serviciilor în conformitate cu prezentul Acord. Prin urmare, Operatorul se angajează să despăgubească și să exonereze de răspundere Împuternicitul pentru orice perturbare, daună sau întrerupere în executarea Prelucrării care ar putea rezulta din inadecvarea, anomaliile și/sau orice disfuncționalități ale Sistemelor Operatorului pe care Împuternicitul este chemat să opereze.

3. OBLIGAȚIILE ÎMPUTERNICITULUI

3.1. În limitele competenței sale în temeiul Contractului și al prezentului Acord, Împuternicitul va fi obligat, pentru sine și pentru Persoanele sale Autorizate, să respecte dispozițiile Legislației Aplicabile, cu referire specială la dispozițiile RGPD, precum și măsurile aplicabile ale Autorităților de Supraveghere competente care impun obligații specifice persoanelor împuternicite;
3.2. În special, Împuternicitul va efectua operațiunile de Prelucrare care i-au fost atribuite în conformitate cu instrucțiunile date de Operator cuprinse în prezentul Acord, precum și cu cele notificate ulterior de Operator în scris, cu un preaviz rezonabil.
3.3. Împuternicitul va efectua operațiunile de Prelucrare funcționale sarcinilor care i-au fost atribuite în conformitate cu prezentul Acord și cu scopurile pentru care Datele cu Caracter Personal sunt colectate și prelucrate. Orice prelucrare care se abate de la prezentul Acord se efectuează numai pe baza instrucțiunilor documentate ale Operatorului sau în cazul în care Împuternicitul este obligat să o efectueze în temeiul dreptului Uniunii sau al dreptului intern; într-un astfel de caz, Împuternicitul informează Operatorul în prealabil, cu excepția cazului în care legea respectivă interzice o astfel de informare.
3.4. Împuternicitul are obligația de a gestiona documentația referitoare la Prelucrarea care i-a fost încredințată prin proceduri adecvate, potrivit unor criterii de eficiență și asigurând păstrarea, nealterarea și regăsirea ușoară a oricărui document relevant pentru respectarea cerințelor impuse de RGPD.
3.5. Împuternicitul pune la dispoziția Operatorului toate informațiile și documentele necesare pentru a demonstra respectarea obligațiilor prevăzute la art. 28 din RGPD și permite și contribuie la activitățile de audit, inclusiv inspecțiile notificate cu un preaviz rezonabil, efectuate de Operator sau de un terț desemnat de Operator, în conformitate cu termenii, limitele și procedurile prevăzute la articolul 10.
3.6. Împuternicitul informează imediat Operatorul dacă, în opinia sa, o instrucțiune încalcă RGPD sau alte dispoziții ale Legislației Aplicabile. De asemenea, Împuternicitul asistă Operatorul, la cererea acestuia, în procedurile în fața Autorității de Supraveghere competente sau a autorității judiciare, în legătură cu activitățile de Prelucrare aflate în competența sa, în special prin punerea la dispoziție a oricăror informații și documente utile pentru a demonstra respectarea obligațiilor prevăzute de Legislația Aplicabilă privind Prelucrarea Datelor cu Caracter Personal.
3.7. Împuternicitul informează Operatorul, la adresa de E-mail de Notificare, fără întârzieri nejustificate și, în orice caz, în termen de 48 (patruzeci și opt) de ore, cu privire la orice obiecție, inspecție sau solicitare obligatorie din punct de vedere juridic din partea unei Autorități de Supraveghere, a unei autorități judiciare sau a altei autorități publice privind Datele cu Caracter Personal prelucrate în numele Operatorului. În cazul unei solicitări de divulgare, Operatorul este informat înainte ca Împuternicitul să îi dea curs și, în măsura permisă de lege, informarea indică autoritatea solicitantă, temeiul juridic, sfera solicitării și Datele cu Caracter Personal vizate. Împuternicitul nu dă curs solicitărilor care nu sunt obligatorii din punct de vedere juridic.

Aceste informații pot fi reținute sau limitate numai în măsura și pentru perioada în care dreptul Uniunii sau dreptul intern aplicabil Împuternicitului ori un ordin obligatoriu emis în temeiul acestuia o interzice din motive importante de interes public. Într-un astfel de caz, Împuternicitul documentează restricția, divulgă numai Datele cu Caracter Personal strict necesare și informează Operatorul de îndată ce restricția încetează să se aplice. Solicitările autorităților din țări terțe se evaluează, de asemenea, în temeiul art. 48 și al Capitolului V din RGPD.

3.8. Împuternicitul identifică, în cadrul structurii sale organizaționale, Persoanele Autorizate să efectueze operațiuni de Prelucrare a Datelor cu Caracter Personal. La desemnare, Împuternicitul furnizează Persoanelor Autorizate instrucțiuni scrise adecvate privind metodele de Prelucrare, cu respectarea dispozițiilor art. 29 din RGPD și ale prezentului Acord. Cu titlu de exemplu și fără caracter exhaustiv, Împuternicitul, la desemnarea în scris a Persoanelor Autorizate, prevede ca acestea să aibă acces numai la Datele cu Caracter Personal a căror cunoaștere este strict necesară pentru îndeplinirea sarcinilor atribuite (principiul necesității de a cunoaște). Împuternicitul trebuie, de asemenea, să verifice că Persoanele Autorizate aplică toate măsurile de securitate referitoare la păstrarea credențialelor de acces în cazul Prelucrării efectuate prin mijloace electronice. Împuternicitul verifică, de asemenea, că Persoanele Autorizate stochează în siguranță suporturile non-IT care conțin orice copie a Datelor cu Caracter Personal, în special dacă aparțin Categoriilor Speciale. În sfârșit, Împuternicitul se asigură că Persoanele Autorizate sunt ținute de obligații de confidențialitate efective, inclusiv pentru perioada ulterioară încetării raportului de muncă cu Împuternicitul, în legătură cu operațiunile de Prelucrare a Datelor cu Caracter Personal efectuate de acestea.

3.9. Între Părți, în cazul unor prejudicii rezultate din Prelucrare, Împuternicitul răspunde în temeiul art. 82 din RGPD numai în măsura în care prejudiciile sunt cauzate de o încălcare care îi este imputabilă a obligațiilor din RGPD care se adresează în mod specific persoanelor împuternicite sau de faptul că a acționat în afara instrucțiunilor legale ale Operatorului ori contrar acestora. Răspunderea Împuternicitului este limitată la partea din prejudiciu corespunzătoare contribuției sale efective la producerea acestuia și este supusă limitărilor de răspundere prevăzute în Acord.

3.10. Acolo unde este cazul și în măsura impusă de legile, reglementările sau măsurile obligatorii ale Autorității de Supraveghere competente aplicabile Serviciului relevant sau Entității Prestatoare, Împuternicitul va implementa măsuri adecvate pentru identificarea, autorizarea, instruirea și monitorizarea personalului cu acces privilegiat sau administrativ la sistemele utilizate pentru Prelucrarea Datelor cu Caracter Personal. Orice cerințe specifice fiecărei țări, inclusiv cerințele privind administratorii de sistem, vor fi prevăzute în Fișa de Prelucrare relevantă.

3.11. În conformitate cu articolul 28 alineatul (3) litera (a) din RGPD, Operatorul include printre instrucțiunile adresate Împuternicitului executarea operațiunilor de prelucrare strict necesare pentru următoarele activități menite să îmbunătățească Serviciile acoperite de Contract: testarea, măsurarea și optimizarea performanței, calibrarea și validarea modelelor/algoritmilor, îmbunătățirea preciziei/fiabilității/utilizabilității, securitatea și prevenirea fraudei, corectarea erorilor și anomaliilor, în măsura în care acestea sunt funcționale pentru furnizarea corespunzătoare a Serviciilor către Operator. Este exclusă orice utilizare în scopuri autonome ale Împuternicitului sau ale Subîmputerniciților săi, inclusiv marketing, profilare sau dezvoltarea de produse/servicii fără legătură.

3.12. Activitățile de îmbunătățire menționate în paragraful precedent se vor desfășura numai în măsura strict necesară pentru furnizarea, întreținerea și securitatea Serviciilor sau, în caz contrar, pe date anonimizate/agregate, cu excepția cazului în care Operatorul dispune altfel, în mod justificat legal. Împuternicitul poate angaja Subîmputerniciți, cu condiția să impună interdicția reutilizării datelor și a antrenării de modele de uz general, precum și obligația de a șterge datele la finalizarea activităților.

4. SECURITATEA PRELUCRĂRII

4.1. În limitele competenței sale în temeiul Contractului și al prezentului Acord, Împuternicitul are obligația, pentru sine și pentru Persoanele sale Autorizate, să pună în aplicare Măsurile de Securitate prevăzute de Legislația Aplicabilă, precum și cele indicate de Operator, asistându-l pe acesta din urmă în asigurarea conformității cu art. 32 din RGPD.

4.2. În contextul activităților de prelucrare a Datelor cu Caracter Personal legate de furnizarea Serviciilor, Furnizorul se angajează să adopte măsuri tehnice și organizatorice adecvate pentru a preveni prelucrarea ilegală sau neautorizată, precum și pentru a proteja Datele cu Caracter Personal împotriva distrugerii, modificării, pierderii, accesului neautorizat sau divulgării, astfel cum se detaliază **în Anexa II – Măsuri Tehnice și Organizatorice de Securitate** la prezentul Acord.

4.3. **Anexa II** descrie măsurile adoptate de Furnizor pentru a asigura confidențialitatea, integritatea, disponibilitatea și reziliența sistemelor și Serviciilor, precum și procedurile pentru restabilirea în timp util a accesului la Datele cu Caracter Personal în cazul unui incident de securitate. Măsurile implementate („**Măsurile de Securitate**”) sunt definite în raport cu nivelul de risc asociat Datelor cu Caracter Personal prelucrate, luând în considerare stadiul actual al tehnologiei, costurile de implementare, precum și natura, contextul și scopurile prelucrării. Clientul recunoaște și este de acord că aceste măsuri sunt adecvate pentru a asigura un nivel de securitate conform cu cerințele de reglementare aplicabile, fără a aduce atingere obligațiilor Furnizorului prevăzute la art. 32 din RGPD.

4.4. Furnizorul își rezervă dreptul de a actualiza sau modifica Măsurile de Securitate pentru a asigura adaptarea constantă la evoluțiile tehnologice și de reglementare, cu condiția ca aceste modificări să nu reducă nivelul general de protecție al Serviciilor.

4.5. În cazul în care Clientul solicită adoptarea unor măsuri de securitate suplimentare specifice, pe lângă cele prevăzute, Furnizorul va evalua fezabilitatea tehnică și operațională a acestor solicitări, rezervându-și posibilitatea de a aplica costuri suplimentare pentru eventualele implementări.

4.6. În cazul produselor instalate la sediul Clientului sau la sediul unor terți desemnați de Client (de exemplu, soluții on-premises), Măsurile de Securitate adoptate de Furnizor se vor aplica exclusiv Serviciilor care implică prelucrarea Datelor cu Caracter Personal de către Furnizor sau de către subîmputerniciții săi (de exemplu, activități de asistență și suport la distanță sau servicii de migrare).

4.7. În cazul în care Serviciile permit integrarea cu software sau aplicații ale terților, Furnizorul nu va fi responsabil pentru Măsurile de Securitate aplicate de aceste părți sau pentru eventualele vulnerabilități rezultate din integrarea efectuată direct de Client sau de furnizori terți, cu excepția cazului în care integrarea a fost furnizată de Furnizor.

4.8. Fără a aduce atingere obligațiilor de securitate ale Furnizorului, Clientul este responsabil de adoptarea tuturor măsurilor necesare pentru a asigura protecția Datelor cu Caracter Personal prelucrate în contextul utilizării Serviciilor de către personalul său sau de către orice părți autorizate.

4.9. Clientul se angajează să utilizeze Serviciile în conformitate cu cele mai bune practici de securitate și să asigure un nivel adecvat de protecție împotriva riscurilor asociate prelucrării Datelor cu Caracter Personal.

4.10. Clientul trebuie să implementeze toate măsurile adecvate pentru a proteja credențialele de autentificare, dispozitivele și sistemele utilizate pentru accesarea Serviciilor, precum și pentru a efectua copii de siguranță periodice ale Datelor cu Caracter Personal, în scopul asigurării restaurării acestora în conformitate cu reglementările aplicabile, sub rezerva oricăror obligații de efectuare a copiilor de siguranță și de restaurare asumate în mod expres de Furnizor.

4.11. Furnizorul nu va fi responsabil pentru protecția Datelor cu Caracter Personal pe care Clientul sau terții le prelucrează în afara sistemelor Furnizorului și ale subîmputerniciților săi, inclusiv datele stocate pe hârtie sau pe infrastructurile IT interne ale Clientului (de exemplu, centre de date private sau servere on-premises).

5. SUBÎMPUTERNICITUL

5.1. Exclusiv în scopul furnizării Serviciilor care fac obiectul Contractului și în conformitate cu prevederile prezentului Acord, Datele cu Caracter Personal pot fi prelucrate de Subîmputerniciți identificați de Împuternicit.
5.2. Împuternicitul poate recurge, pentru furnizarea efectivă a unuia sau mai multor Servicii, la alte societăți aparținând Grupului Namirial. Societatea din Grupul Namirial care furnizează efectiv un anumit Serviciu („Entitatea Prestatoare") este identificată, pentru fiecare Serviciu, în Fișa de Prelucrare relevantă. Atunci când Entitatea Prestatoare nu coincide cu Împuternicitul, aceasta va opera în temeiul unor acorduri intra-grup între societățile Grupului Namirial, conforme cu articolul 28 din RGPD, preexistente și separate de prezentul Acord. Operatorul ia cunoștință de acest lucru prin semnarea prezentului Acord. Atunci când Entitatea Prestatoare coincide cu Împuternicitul, Subîmputerniciții enumerați în Fișa de Prelucrare sunt contractați direct de către Împuternicit. În orice caz, Împuternicitul va rămâne pe deplin răspunzător față de Operator pentru activitățile de Prelucrare efectuate de Entitatea Prestatoare și de Subîmputerniciții acesteia în numele Operatorului în temeiul prezentului Acord.
5.3. Orice activitate de prelucrare pentru care Entitatea Prestatoare acționează într-un rol diferit în materie de protecție a datelor va fi identificată în Fișa de Prelucrare relevantă și nu va fi guvernată de prezentul Acord, cu excepția cazurilor prevăzute în mod expres.
5.4. Împuternicitul se angajează să își selecteze Subîmputerniciții dintre persoanele a căror experiență, capacitate și fiabilitate oferă garanții suficiente pentru implementarea unor Măsuri de Securitate adecvate, astfel încât Prelucrarea să îndeplinească toate cerințele Legislației Aplicabile și să asigure protecția drepturilor Persoanei Vizate. În consecință, Împuternicitul se angajează să încheie contracte specifice sau alte acte juridice obligatorii cu Subîmputerniciții, prin care Împuternicitul descrie în detaliu sarcinile acestora și le impune respectarea acelorași obligații impuse de Operator Împuternicitului în temeiul Legislației Aplicabile și al prezentului Acord.
5.5. În orice caz în care un Subîmputernicit nu își respectă obligațiile privind protecția Datelor cu Caracter Personal, Împuternicitul recunoaște că își păstrează întreaga răspundere față de Operator pentru conduita respectivului Subîmputernicit. În consecință, Împuternicitul se angajează să despăgubească și să exonereze de răspundere Operatorul pentru orice prejudicii, reclamații și cereri de despăgubire care ar putea fi formulate împotriva Operatorului ca urmare a nerespectării de către Subîmputernicit a obligațiilor sale și, în general, a oricărei încălcări a Legislației Aplicabile de către Subîmputernicit și de către oricare dintre subcontractanții și/sau persoanele autorizate ale acestuia.
5.6. Fișele de Prelucrare identifică și enumeră Subîmputerniciții desemnați de Împuternicit și deja aprobați de Operator. Împuternicitul se angajează, de asemenea, să informeze Operatorul în scris cu privire la orice modificări sau înlocuiri planificate privind Subîmputerniciții, oferind Operatorului posibilitatea de a se opune acestor modificări în termen de 30 (treizeci) de zile de la primirea comunicării relevante.
5.7. Comunicarea menționată în paragraful precedent poate fi realizată, în mod alternativ, prin publicarea listei actualizate a Subîmputerniciților în secțiunea „Documentație" de pe site-ul web al Furnizorului, accesibil prin datele de contact indicate în Anexa A la Condițiile Generale.

6. TRANSFERUL DATELOR CU CARACTER PERSONAL

6.1. Împuternicitul declară că nu va transfera Date cu Caracter Personal în afara SEE, cu excepția cazului în care este autorizat în prealabil și în mod specific, în scris, de către Operator. În cazul autorizării, Împuternicitul poate transfera Date cu Caracter Personal numai pe baza instrucțiunilor documentate ale Operatorului și, în special, cu respectarea deplină a art. 44, 45, 46 și 49 din RGPD. Transferurile și Subîmputerniciții din afara SEE indicați în Fișa de Prelucrare semnată de Părți se consideră autorizați.

6.2. În cazul în care un transfer către o țară terță sau o organizație internațională este impus de dreptul Uniunii sau de dreptul intern la care este supus Împuternicitul, fără o instrucțiune specifică a Operatorului, se aplică obligațiile de notificare, verificare și documentare prevăzute la art. 3.7, împreună cu art. 48, după caz, și cu Capitolul V din RGPD.

6.3. În orice caz de transfer de Date cu Caracter Personal în afara SEE, în măsura în care nu există o Decizie de Adecvare a Comisiei Europene pentru țara de destinație a Datelor cu Caracter Personal, Împuternicitul este obligat să semneze și să solicite destinatarilor Datelor cu Caracter Personal să semneze Clauzele Contractuale Standard în ultima lor versiune adoptată de Comisia Europeană, asigurându-se că aceleași obligații cuprinse în acestea sunt garantate față de orice destinatari ulteriori ai Datelor cu Caracter Personal în cazul așa-numitului transfer ulterior (onward transfer). Dacă și acolo unde este necesar, Împuternicitul trebuie să stipuleze, de asemenea, adoptarea oricăror Măsuri de Securitate suplimentare în conformitate cu Recomandările 01/2020 privind măsurile care completează instrumentele de transfer pentru a asigura conformitatea cu nivelul UE de protecție a Datelor cu Caracter Personal, precum și cu orientările aplicabile ale Comitetului European pentru Protecția Datelor („CEPD”).

7. ASISTENȚĂ ACORDATĂ OPERATORULUI

7.1. Ținând seama de natura Prelucrării și de informațiile de care dispune, Împuternicitul este obligat să acorde sprijin Operatorului, astfel încât acesta din urmă să își poată îndeplini obligațiile impuse de Legislația Aplicabilă operatorilor de date, cum ar fi, cu titlu de exemplu și fără caracter exhaustiv, obligațiile de a:

a. notifica o Încălcare a Securității Datelor cu Caracter Personal Autorității de Supraveghere competente, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la luarea la cunoștință, cu excepția cazului în care este puțin probabil ca încălcarea să genereze un risc pentru drepturile și libertățile persoanelor fizice;
b. efectua o evaluare de impact asupra protecției datelor (DPIA) în legătură cu Prelucrarea reglementată de prezentul Acord, dacă respectiva Prelucrare prezintă caracteristicile prevăzute la art. 35 din RGPD;
c. consulta Autoritatea de Supraveghere competentă în conformitate cu art. 36 din RGPD, în cazul în care o DPIA indică faptul că Prelucrarea reglementată de prezentul Acord ar genera un risc ridicat în absența unor măsuri de atenuare a riscului;
d. răspunde la cererile de exercitare a Drepturilor Persoanelor Vizate, în conformitate cu capitolul III din RGPD. În cazul în care Împuternicitul primește astfel de cereri în mod direct, acesta (i) va informa cu promptitudine Operatorul în scris, atașând o copie a cererii; și (ii) ținând seama de natura Prelucrării, va asista Operatorul cu măsuri tehnice și organizatorice adecvate, în limita competenței sale, pentru soluționarea acestor cereri.

8. ÎNCĂLCĂRI ALE SECURITĂȚII DATELOR CU CARACTER PERSONAL

8.1. În cazul în care Împuternicitul ia cunoștință de o Încălcare a Securității Datelor cu Caracter Personal care implică sau ar putea implica, chiar și indirect, sistemele și operațiunile de Prelucrare utilizate în numele Operatorului sau Datele cu Caracter Personal care fac obiectul prezentului Acord, Împuternicitul se angajează să informeze Operatorul printr-o comunicare formală transmisă la adresa de E-mail de Notificare, fără întârzieri nejustificate și în termen de cel mult 24 (douăzeci și patru) de ore de la luarea la cunoștință a Încălcării Securității Datelor cu Caracter Personal.

8.2. După detectarea unei anomalii sau a unei suspiciuni de Încălcare a Securității Datelor cu Caracter Personal acoperite de prezentul Acord, Împuternicitul este obligat să inițieze o analiză preliminară pentru a colecta date referitoare la anomalie și, în orice caz, toate informațiile necesare pentru clasificarea și gestionarea încălcării, inclusiv detalii referitoare la natura incidentului, datele implicate, măsurile luate și timpii de intervenție.

8.3. Împuternicitul se angajează să asigure respectarea termenelor menționate mai sus și să despăgubească și să exonereze de răspundere Operatorul pentru orice prejudicii, reclamații și cereri de despăgubire care ar putea fi formulate împotriva Operatorului ca urmare a nerespectării de către Împuternicit a obligațiilor sale și, în general, a oricărei încălcări a Legislației Aplicabile de către Împuternicit și de către oricare dintre subcontractanții și/sau persoanele autorizate ale acestuia.

8.4. În cazul unei Încălcări a Securității Datelor cu Caracter Personal, Împuternicitul se angajează să ofere, în limita competenței și responsabilității sale în temeiul Contractului, cooperarea maximă Operatorului și Autorităților de Supraveghere competente, în vederea îndeplinirii oricăror obligații legale aplicabile (de exemplu, obligația de notificare către Autoritatea de Supraveghere, eventuala informare a Persoanelor Vizate, aplicarea măsurilor adecvate pentru atenuarea sau prevenirea riscurilor și a prejudiciilor). În acest sens, Operatorul se angajează să furnizeze cu promptitudine Împuternicitului dovada oricărei comunicări purtate cu Autoritățile de Supraveghere competente în care Împuternicitul este implicat sau menționat în orice mod.

9. DURATA. ȘTERGEREA ȘI RETURNAREA DATELOR CU CARACTER PERSONAL

9.1. Desemnarea ca persoană împuternicită în temeiul prezentului Acord va avea aceeași durată ca și Contractul, cu excepția revocării anterioare, caz în care desemnarea va continua să producă efecte atât cât este necesar pentru finalizarea operațiunilor de Prelucrare necesare încetării raportului dintre Părți sau pentru îndeplinirea obligațiilor legale care le revin.

9.2. La încetarea operațiunilor de Prelucrare încredințate, precum și la încetarea, din orice motiv, a raportului contractual cu Împuternicitul, acesta din urmă, la alegerea Operatorului, va fi obligat (i) să returneze Operatorului Datele cu Caracter Personal care fac obiectul Prelucrării sau (ii) să procedeze la distrugerea completă a Datelor cu Caracter Personal și a fiecărei copii a acestora, cu excepția cazurilor în care păstrarea datelor este impusă de dreptul Uniunii sau de dreptul intern (de exemplu, obligații contabile sau fiscale) ori este necesară pentru constatarea, exercitarea sau apărarea unor drepturi în justiție. Datele păstrate în temeiul excepțiilor de mai sus, precum și copiile de siguranță care nu pot fi șterse imediat din motive tehnice, se păstrează în formă protejată, nu fac obiectul altor prelucrări și se șterg la expirarea perioadei de păstrare aplicabile sau în conformitate cu ciclurile normale de suprascriere. În ambele cazuri, Împuternicitul furnizează Operatorului o declarație scrisă care confirmă returnarea sau ștergerea, cu indicarea eventualelor excepții menționate mai sus.

10. AUDIT ȘI INSPECȚII

10.1. Împuternicitul pune la dispoziția Operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor sale în temeiul prezentului Acord și al Legislației Aplicabile și va permite și va contribui la activitățile de audit, inclusiv inspecțiile efectuate de Operator și/sau de un terț desemnat de Operator.

10.2. Activitățile de audit se vor desfășura, de preferință, în format documentar sau pe bază de interviuri, inclusiv prin chestionare, solicitări de informații, analiza certificărilor, a rapoartelor de audit, a politicilor, procedurilor și a altor documente de conformitate puse la dispoziție de Împuternicit.

10.3. Cu excepția cazului unei Încălcări a Securității Datelor cu Caracter Personal cu impact semnificativ asupra Datelor cu Caracter Personal prelucrate în numele Operatorului sau al cazului în care o Autoritate de Supraveghere competentă a emis o sancțiune sau o măsură obligatorie împotriva Împuternicitului direct legată de Servicii, Operatorul:

(a) va transmite Împuternicitului o notificare scrisă prealabilă de cel puțin treizeci (30) de zile;
(b) va efectua cel mult un audit pe an calendaristic;
(c) se va asigura că auditul nu depășește două (2) zile lucrătoare întregi; și
(d) va desfășura auditul într-un mod care să nu perturbe în mod nerezonabil activitatea comercială obișnuită a Împuternicitului.

10.4. Operatorul va suporta toate costurile, cheltuielile și onorariile aferente auditului, inclusiv eventualele costuri ale auditorilor desemnați de Operator. În cazul în care auditul necesită timp sau resurse care depășesc limitele prevăzute la articolul 10.3, Împuternicitul va informa Operatorul în prealabil, iar Părțile vor conveni cu bună-credință fie reducerea sferei auditului, fie alocarea costurilor suplimentare în sarcina Operatorului.

10.5. Atunci când auditul se desfășoară prin chestionare, formulare sau solicitări documentare, Împuternicitului i se va acorda un termen rezonabil de răspuns, care nu va fi mai scurt de treizeci (30) de zile de la primirea solicitării complete. Acest termen poate fi prelungit atunci când este necesar în mod rezonabil, ținând seama de complexitatea solicitării și de disponibilitatea personalului Împuternicitului.

10.6. Operatorul și orice terț desemnat de acesta vor utiliza informațiile obținute în cursul auditului exclusiv în scopul verificării conformității cu prezentul Acord și vor păstra aceste informații strict confidențiale.

11. COMUNICĂRI ÎNTRE PĂRȚI

11.1. În sensul prezentului Acord, Împuternicitul declară că a numit un responsabil cu protecția datelor (DPO) și/sau a identificat persoana de contact relevantă pentru protecția datelor, acolo unde este cazul, în conformitate cu Legislația Aplicabilă. Datele de contact relevante ale Împuternicitului, inclusiv datele DPO-ului sau ale persoanei de contact pentru protecția datelor, sunt cele indicate pentru Furnizorul relevant în Anexa A la Condițiile Generale, astfel cum este identificat în Oferta Comercială. Aceste date de contact vor fi utilizate pentru toate comunicările referitoare la confidențialitate și protecția datelor în temeiul prezentului Acord.

11.2. Împuternicitul va contacta Operatorul, în toate cazurile prevăzute în prezentul Acord, prin comunicare transmisă la adresa de E-mail de Notificare furnizată de Operator.

11.3. Părțile se angajează să își notifice reciproc, cu promptitudine, orice modificare a adreselor lor de contact. În absența unei astfel de notificări în timp util, comunicările trimise la adresa neactualizată vor fi considerate valabile și efective.

ANEXA I

DEFINIȚII

a) „**Acord”** înseamnă prezentul Acord privind Prelucrarea Datelor, inclusiv preambulul și Anexele;
b) „**Administratori de Sistem”** înseamnă Persoanele Autorizate responsabile de gestionarea și întreținerea unui sistem de prelucrare sau a componentelor acestuia, identificate în conformitate cu art. 32 din RGPD și cu cerințele naționale aplicabile privind atribuirea funcțiilor de administrator de sistem, astfel cum sunt detaliate, după caz, în Fișa de Prelucrare aplicabilă;
c) „**Autoritate de Supraveghere”** înseamnă orice autoritate de supraveghere independentă în temeiul capitolului VI din RGPD, competentă să monitorizeze și să asigure aplicarea dispozițiilor legale privind protecția Datelor cu Caracter Personal, cu referire la Prelucrarea Datelor cu Caracter Personal efectuată în executarea Contractului (pentru România, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal – ANSPDCP);
d) **„Categorii Speciale de Date cu Caracter Personal”** înseamnă Datele cu Caracter Personal care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filozofice ori apartenența la sindicate, precum și prelucrarea datelor genetice, a datelor biometrice destinate identificării unice a unei persoane fizice, a datelor privind sănătatea sau a datelor privind viața sexuală ori orientarea sexuală a unei persoane fizice, astfel cum sunt identificate la art. 9 din RGPD;
e) **„Clauze Contractuale Standard”** înseamnă clauzele adoptate de Comisia Europeană prin Decizia 2021/914/UE din 4 iunie 2021 pentru transferul Datelor cu Caracter Personal de la un operator de date stabilit în Uniunea Europeană („UE”) / Spațiul Economic European („SEE”) către o entitate din afara UE sau a SEE care acționează în calitate de persoană împuternicită;
f) **„Contract”** înseamnă contractul semnat între Părți pentru furnizarea Serviciilor;
g) **„Date cu Caracter Personal”** înseamnă orice informații referitoare la o persoană fizică identificată sau identificabilă („Persoana Vizată”), prelucrate de Împuternicit, în numele Operatorului, în legătură cu executarea Contractului;
h) **„Drepturile Persoanei Vizate”** înseamnă drepturile recunoscute Persoanei Vizate de Legislația Aplicabilă. În limitele aplicabilității RGPD, „Drepturile Persoanei Vizate” înseamnă, de exemplu, dreptul de a solicita operatorului de date accesul la Datele cu Caracter Personal, rectificarea sau ștergerea acestora, dreptul la restricționarea Prelucrării datelor Persoanei Vizate sau dreptul de a se opune Prelucrării, precum și dreptul la portabilitatea datelor;
i) **„E-mail de Notificare”** înseamnă adresa (sau adresele) de e-mail furnizată (furnizate) de Client la momentul semnării Contractului sau furnizată (furnizate) Împuternicitului prin alt canal oficial, la care Clientul intenționează să primească notificări de la Împuternicit;
j) **„Legislație Aplicabilă”** înseamnă toate legile și reglementările privind protecția Datelor cu Caracter Personal aplicabile Prelucrării Datelor cu Caracter Personal în temeiul Contractului, inclusiv Regulamentul (UE) 2016/679 („RGPD”), orice legi și reglementări naționale aplicabile în materie de protecție a datelor ale statelor membre UE (pentru România, inclusiv Legea nr. 190/2018), potrivit domeniului lor teritorial și de aplicare, precum și orice măsuri, decizii, orientări sau instrucțiuni obligatorii emise de Autoritatea de Supraveghere competentă;
k) **„Măsuri de Securitate”** înseamnă măsurile tehnice și organizatorice, conform art. 32 din RGPD, adecvate pentru a asigura un nivel corespunzător de securitate a Datelor cu Caracter Personal, precum și toate măsurile necesare pentru a preveni sau cel puțin a minimiza orice risc previzibil în mod rezonabil de distrugere, pierdere, modificare, divulgare sau acces neautorizat, accidental sau ilegal, asupra Datelor cu Caracter Personal prelucrate;
l) **„Persoane Autorizate”** înseamnă persoanele fizice din cadrul structurii organizaționale a Împuternicitului, identificate în mod specific în scris și autorizate să acceseze și să prelucreze Datele cu Caracter Personal în contextul executării Contractului, care acționează sub controlul și potrivit instrucțiunilor Împuternicitului;
m) **„Persoană împuternicită de operator”** înseamnă, în general, persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează Date cu Caracter Personal în numele unui operator de date;
n) **„Servicii”** înseamnă serviciile furnizate în temeiul Contractului;
o) **„Sistemele Operatorului”** înseamnă infrastructurile și sistemele eventual puse la dispoziție de Operator și/sau de terți desemnați de acesta, pe care Împuternicitul este chemat să efectueze Prelucrarea;
p) **„Subîmputernicit”** înseamnă o entitate identificată de Împuternicit care efectuează, în totalitate sau parțial, Prelucrarea Datelor cu Caracter Personal încredințată Împuternicitului,

cu respectarea obligațiilor și instrucțiunilor stabilite de Operator, și care a fost autorizată în mod expres de acesta din urmă;

q) „**Subîmputernicit Intra-Grup**” înseamnă societatea aparținând Grupului Namirial care acționează ca Subîmputernicit pentru furnizarea efectivă a unuia sau mai multor Servicii, în temeiul unor acorduri intra-grup preexistente între societățile Grupului Namirial, conforme cu articolul 28 din RGPD și separate de prezentul Acord;

r) „**Entitate Prestatoare**” înseamnă societatea din Grupul Namirial care furnizează efectiv Serviciul specific acoperit de fiecare Fișă de Prelucrare. Entitatea Prestatoare poate coincide cu Împuternicitul sau poate opera ca Subîmputernicit Intra-Grup al acestuia. În ambele cazuri, aceasta este identificată în Fișa de Prelucrare relevantă;

s) **„Operator”** înseamnă, în general, persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele prelucrării Datelor cu Caracter Personal;

t) **„Prelucrare”** înseamnă orice operațiune sau set de operațiuni efectuate asupra Datelor cu Caracter Personal sau asupra seturilor de Date cu Caracter Personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.

ANEXA II

MĂSURI TEHNICE ȘI ORGANIZATORICE DE SECURITATE

1. MĂSURI DE SECURITATE ORGANIZATORICE

TIPUL MĂSURII	DESCRIERE
Politici și regulamente interne	Împuternicitul a adoptat un set de politici, proceduri și reglementări interne, obligatorii pentru tot personalul autorizat să prelucreze Date cu Caracter Personal. Aceste politici și linii directoare definesc regulile pentru utilizarea în siguranță a resurselor IT și prevăd reglementări interne specifice pentru gestionarea informațiilor, cu respectare obligatorie de către toți utilizatorii. Obiectivul este asigurarea respectării principiilor de confidențialitate, integritate și disponibilitate a Datelor cu Caracter Personal, minimizând riscurile de acces neautorizat sau de utilizare abuzivă a informațiilor în cadrul tuturor societăților din grup.
Autorizarea accesului și controale logice	Împuternicitul definește profilurile de acces cu respectarea privilegiilor minime necesare pentru îndeplinirea sarcinilor atribuite. Profilurile de autorizare sunt identificate și configurate înainte de începerea prelucrării, pentru a limita accesul numai la Datele cu Caracter Personal necesare efectuării operațiunilor de prelucrare. Pentru operațiunile mai sensibile se adoptă autentificarea cu doi factori (MFA), pentru a consolida securitatea accesului. Aceste profiluri sunt supuse unor verificări periodice pentru a se verifica menținerea condițiilor necesare păstrării profilurilor atribuite.
Monitorizarea accesului	Accesul la sistemele de prelucrare a Datelor cu Caracter Personal este înregistrat și monitorizat, cu analiza periodică a jurnalelor pentru identificarea eventualelor anomalii sau activități suspecte.
Gestionarea schimbărilor	Împuternicitul a adoptat o procedură specifică ce reglementează procesul de gestionare a schimbărilor, ținând cont de introducerea oricăror inovații tehnologice sau modificări în structura sa organizațională.
Gestionarea incidentelor și continuitatea activității	Împuternicitul a implementat o procedură specifică de gestionare a incidentelor pentru a asigura restabilirea cât mai rapidă a funcționării normale a serviciilor, menținând cele mai bune niveluri de servicii. Incidentele sunt clasificate în funcție de gravitate și de impactul asupra Datelor cu Caracter Personal. Personalul este instruit să gestioneze evenimentele de securitate și să execute proceduri de izolare. Se efectuează teste periodice privind capacitatea de reacție a organizației la incidente. Este implementat un Plan de Continuitate a Activității pentru a asigura reziliența serviciilor chiar și în situații de urgență.
Măsuri pentru asigurarea păstrării limitate a datelor	Împuternicitul respectă principiile protecției datelor începând cu momentul conceperii și în mod implicit. Măsuri tehnice: nu se colectează mai multe Date cu Caracter Personal decât este necesar pentru scopul respectiv; utilizarea unor setări implicite care respectă protecția datelor. Măsuri organizatorice: politica de protecție a datelor conform principiilor „privacy by design / by default”, inclusă în Politica de Confidențialitate și Protecție a Datelor cu Caracter Personal a Grupului SCS-P14; se efectuează verificări de securitate OWASP Secure Mobile Development (a se vedea Politica de Codificare Securizată a Grupului SCS-P08);

	analiza perimetrală a aplicațiilor web.
Încălcarea securității datelor	Împuternicitul a implementat o procedură specifică pentru gestionarea evenimentelor și incidentelor cu impact potențial asupra Datelor cu Caracter Personal, definind rolurile și responsabilitățile, procesul de detectare (suspectată sau confirmată), aplicarea contramăsurilor, răspunsul și limitarea incidentului/încălcării, precum și metodele de comunicare promptă către Operator a încălcărilor securității Datelor cu Caracter Personal. Din partea Împuternicitului, această procedură identifică cel puțin: natura încălcării securității Datelor cu Caracter Personal, inclusiv, dacă este posibil, categoriile și numărul aproximativ de persoane vizate, precum și categoriile și numărul aproximativ de înregistrări de Date cu Caracter Personal implicate; consecințele probabile ale încălcării; măsurile luate sau propuse pentru remedierea încălcării și, după caz, pentru atenuarea posibilelor sale efecte negative.
Formare	Pentru a asigura un nivel adecvat de conștientizare, Împuternicitul oferă instruire periodică privind prelucrarea corectă a Datelor cu Caracter Personal și securitatea informațiilor. Instruirea este obligatorie pentru tot personalul care are acces la Date cu Caracter Personal. Se efectuează teste și verificări pentru a evalua nivelul de înțelegere a politicilor de securitate. Se organizează campanii simulate de atacuri cibernetice (de exemplu, teste de phishing) pentru a educa personalul cu privire la amenințările comune. Instruirea este actualizată periodic pentru a reflecta evoluțiile normative și tehnologice.
Gestionarea Subîmputerniciților	Atunci când Împuternicitul utilizează Subîmputerniciți, se implementează controale stricte pentru a verifica conformitatea acestora cu măsurile de securitate necesare. Fiecare Subîmputernicit trebuie să respecte standarde de securitate echivalente cu cele ale Împuternicitului. Se efectuează audituri și inspecții periodice pentru a verifica conformitatea furnizorilor. Împuternicitul menține un registru actualizat al Subîmputerniciților.
Copii de siguranță și recuperarea datelor	Pentru a asigura disponibilitatea datelor și rezistența la defecțiuni, Împuternicitul implementează un sistem de copii de siguranță și de recuperare în caz de dezastru care include: copii de siguranță periodice cu politici de păstrare definite; protecția copiilor de siguranță prin criptare și acces controlat; teste periodice pentru a asigura recuperarea rapidă a datelor atunci când este necesar; replicarea datelor în centre de date securizate pentru a preveni pierderea informațiilor critice.
Proceduri de testare, verificare și evaluare periodică a eficacității măsurilor tehnice și organizatorice pentru asigurarea securității prelucrării	Politicile interne referitoare la măsurile de securitate sunt revizuite periodic și confirmate în ceea ce privește adecvarea și eficacitatea în cadrul auditurilor interne în derulare și, anual, de către organisme de certificare independente, externe și acreditate, în cadrul auditurilor de monitorizare și recertificare ISO 9001 și ISO 27001.
Numirea CISO	Pentru a asigura un nivel adecvat de securitate a informațiilor și conformitatea cu reglementările aplicabile, Împuternicitul a numit un Chief Information Security Officer (CISO) cu sarcina principală de a: supraveghea implementarea și eficacitatea măsurilor de securitate adoptate pentru protecția Datelor cu Caracter Personal; monitoriza evoluția amenințărilor cibernetice și promova actualizarea continuă a politicilor de securitate; coordona activitățile de răspuns la incidentele de securitate; defini strategii de îmbunătățire a securității pentru protecția activelor societății. CISO operează în sinergie cu celelalte funcții corporative implicate în gestionarea securității

	și a protecției datelor.
Certificări de conformitate	Lista completă a certificărilor deținute de Furnizor este disponibilă la următoarea adresă: https://www.namirial.com/en/company/certifications/

2. MĂSURI TEHNICE DE SECURITATE

TIPUL MĂSURII	DESCRIERE
Planificarea capacității și monitorizarea performanței	Împuternicitul implementează un proces continuu de analiză și optimizare a resurselor IT pentru a asigura performanța adecvată pentru furnizarea Serviciilor și gestionarea Datelor cu Caracter Personal. Sistemul include monitorizarea proactivă a capacității de prelucrare, a stocării și a lățimii de bandă a rețelei. Nevoile viitoare sunt proiectate pentru a asigura scalabilitatea și continuitatea operațională. Se efectuează teste periodice de încărcare și reziliență pentru a preveni problemele cauzate de suprasolicitări sau de vârfuri de utilizare.
Securitatea și consolidarea sistemelor	Pentru a minimiza vulnerabilitățile și a îmbunătăți protecția infrastructurii IT, Împuternicitul aplică măsuri de consolidare (hardening) sistemelor de operare, software-ului de aplicații și rețelelor societății. Sistemele sunt configurate conform celor mai bune practici de securitate pentru a limita expunerea la riscuri. Funcționalitățile inutile sunt dezactivate, iar accesul la serviciile de rețea este restricționat. Configurațiile sunt revizuite și actualizate periodic în funcție de evoluția amenințărilor.
Gestionarea patch-urilor și actualizările de securitate	Împuternicitul menține un proces structurat de gestionare a actualizărilor pentru a asigura protecția împotriva vulnerabilităților software. Actualizările de securitate sunt aplicate prompt, în funcție de gravitatea vulnerabilităților. Sunt implementate proceduri de testare înainte de lansare pentru a evita impactul negativ asupra continuității serviciului. Sistemele critice sunt supuse unor verificări periodice pentru identificarea eventualelor vulnerabilități nerezolvate.
Protecția rețelei și a sistemelor	Datele cu Caracter Personal sunt protejate prin soluții avansate de securitate perimetrală și de detectare a intruziunilor, inclusiv: firewall-uri de ultimă generație pentru filtrarea avansată a traficului; IDPS (Intrusion Detection & Prevention System) pentru identificarea și blocarea activităților suspecte; segmentarea rețelei pentru a limita riscurile de propagare în cazul unui atac.
Protecția împotriva programelor malware și a amenințărilor cibernetice	Împuternicitul utilizează instrumente avansate de protecție pentru a reduce riscurile generate de malware și de atacurile cibernetice: antivirus și anti-malware actualizate periodic pentru a detecta și bloca amenințările în timp real; sisteme de sandboxing pentru a analiza și izola fișierele suspecte înainte de executare; monitorizarea amenințărilor pentru a preveni atacurile zero-day.
Securitatea comunicațiilor și protecția transmiterii datelor	Împuternicitul adoptă protocoale de securitate avansate pentru a asigura integritatea și confidențialitatea comunicațiilor: criptare end-to-end pentru protejarea datelor în tranzit; autentificare și certificate digitale pentru verificarea integrității comunicațiilor; segmentare VPN și rețele private pentru reducerea riscurilor de interceptare.

Protecția fizică a infrastructurilor IT	Accesul la spațiile în care sunt stocate sau prelucrate Datele cu Caracter Personal este supus unor măsuri de securitate fizică sporite: acces controlat cu sisteme de badge, înregistrarea intrărilor și autorizare prealabilă. Supraveghere video 24/7 și alarme anti-intruziune. Măsuri de securitate a mediului, inclusiv sisteme de protecție împotriva incendiilor, redundanța sistemelor electrice și de climatizare, UPS și generatoare de rezervă pentru asigurarea continuității operaționale. Proceduri de urgență și de recuperare în caz de dezastru, cu simulări periodice pentru testarea planurilor de răspuns la incidente.
Gestionarea credențialelor și accesul la sisteme	Pentru a preveni accesul neautorizat, Împuternicitul implementează un sistem strict de autentificare și de gestionare a credențialelor: autentificare multifactor pentru utilizatorii cu acces la Date cu Caracter Personal și informații sensibile; politică avansată privind parolele, cu cerințe de lungime, complexitate și expirare periodică; revocarea imediată a accesului în cazul încetării raportului de muncă sau al schimbării atribuțiilor.
Gestionarea Administratorilor de Sistem	Administratorii de Sistem, ca persoane cu privilegii ridicate, sunt supuși unui control și unei monitorizări stricte. Împuternicitul menține o listă actualizată și documentată a Administratorilor de Sistem. Activitățile administrative sunt urmărite și înregistrate în jurnale protejate și nealterabile. Se efectuează audituri periodice pentru a verifica acțiunile administratorilor și aplicarea corectă a politicilor de securitate.