Anexa 2 la APD

Măsuri tehnice și organizatorice de securitate

1	**Măsuri generale**

Furnizorul de servicii va implementa măsuri tehnice și organizatorice pentru:

1.1 a se asigura că drepturile de a prelucra Datele cu Caracter Personal Operator sau accesul la acestea sunt acordate numai persoanelor autorizate în mod corespunzător, pe baza principiului de confidențialitate și a necesității de a cunoaște;

În virtutea principiului necesității de a cunoaște, Furnizorul de Servicii, respectiv persoanele autorizate, vor avea acces și vor prelucra numai Datele cu Caracter Personal Operator potrivit APD și a Contractului de Prestări Servicii.

1.2 a preveni/refuza accesul/utilizarea de către persoane neautorizate a zonelor de Prelucrare de Date Operator, inclusiv prin:

1.2.1 spații încuiate accesibile numai persoanelor autorizate să prelucreze date cu caracter personal;

și

1.2.2 Politici de securitate internă și confidențialitate a datelor.

1.3 a se asigura că persoanele implicate în Prelucrarea de Date Operator sunt obligate să respecte angajamentele relevante privind confidențialitatea datelor și că au fost instruite în legătură cu Legea, la cerințele minime de securitate a prelucrărilor de date cu caracter personal, precum și cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal, în funcție de specificul activității persoanei autorizate.

1.4 a se asigura că datele personale nu pot fi citite, copiate, modificate, transferate sau eliminate în mod necorespunzător în timpul transferului sau stocării (electronice) pe un suport de date, inclusiv prin:

1.4.1 Separarea funcțională a datelor personale (stocare, modificare, ștergere, transmitere) în funcție de scopurile pentru care sunt prelucrate; și

1.4.2 asigurarea faptului că Datele cu Caracter Personal Operator sunt accesate numai de persoana/persoanele relevantă(e);

1.5 a preveni/refuza accesul/utilizarea de către persoane neautorizate a sistemelor utilizate pentru Prelucrarea de Date Operator, inclusiv prin:

1.5.1 reglementarea introducerii, modificării, eliminării, gestionării și transferului datelor cu caracter personal din și către sisteme, inclusiv prin intermediul politicilor corespunzătoare ale companiei;

În cazul modificării datelor cu caracter personal, sistemele vor înregistra cine a făcut modificarea, data și ora modificării. Totodată, Furnizorul de Servicii va lua măsuri ca sistemele să mențină datele șterse sau modificate.

1.5.2 o Politică privind conectarea și utilizarea parolelor pentru rețele și conturi de utilizator;

În cadrul acestei reglementări se vor stabili următoarele reguli:

- Fiecare persoană autorizată are propriul său cod de identificare, pe care trebuie sa il tina secret si sa il protejeze ca atare. Niciodată mai multe persoane autorizate nu vor avea același cod de identificare;
- Codurile de identificare (sau conturi de utilizator) nefolosite o perioadă mai îndelungată vor fi dezactivate și distruse;
- La introducerea parolelor acestea nu trebuie să fie afișate în clar pe monitor;
- Sistemul informațional trebuie să refuze automat accesul unui utilizator după 5 introduceri greșite ale parolei;
- Codul de identificare se va revoca sau suspenda, dacă persoana autorizată și-a dat demisia ori a fost concediat, și-a încheiat contractul, a fost transferat la alt serviciu și noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă va absenta o perioadă îndelungată;
- Orice date cu caracter personal vor fi transmise numai daca este cerut de Operator, de Legea aplicabila sau daca este strict necesar pentru îndeplinirea APD si/sau a Contractului de prestări servicii (in acest caz cu respectarea stricta a APD si a Legii) si, in toate cazurile prin parolarea in mod corespunzător a fișierului/documentului/ corespondentei care conține astfel de date (a se vedea regulile din prezenta anexa), iar parola se va transmite destinatarului într-o maniera securizata si separat de documentul/fișierul/corespondenta in cauza.

1.5.3 dezactivarea automată (de ex. desktop blocat după o anumită perioadă de inactivitate – de exemplu 10 minute);

1.5.4 Diferite forme de permisiuni de acces (de exemplu, per rol, per obiect) revizuite periodic;

Scoaterea la imprimantă a datelor cu caracter personal se va realiza numai de persoane autorizate pentru această operațiune de către Furnizorul de Servicii, asigurandu-se in permanenta pastrarea caracterului confidential al acestora.

1.5.5 Drepturi speciale de acces pentru directoarele cu date sensibile;

1.5.6 Limitarea accesului administrativ la platformele firewall la personalul IT; personalul IT va avea acces la datele cu caracter personal, după ce acestea sunt transformate în date anonime

1.5.7 Proceduri de modificare/terminare a accesului logic la directoarele active;

1.5.8 Acordarea unei atenții deosebite datelor care părăsesc zonele de prelucrare, inclusiv prin:

(i) Asigurarea faptului că persoanele care folosesc computere portabile si/sau dispozitive portabile de stocare (hard disck-uri portabile flash drives etc.) cu date personale au grijă deosebită în timpul transportului, depozitării și utilizării dispozitivului în afara zonelor de prelucrare (inclusiv prin criptare);

(ii) Securizarea, pentru a asigura confidențialitatea și integritatea datelor, a dispozitivelor/mediilor de stocare care conțin date personale, inclusiv date sensibile transferate în afara zonelor de prelucrare;

(iii) Eliminarea datelor cu caracter personal de pe suporturile de date care sunt puse la dispoziția persoanelor neautorizate (inclusiv pentru reparare sau distrugere);

1.5.9 Luarea de măsuri specifice cu privire la rețelele publice, inclusiv:

(i) Securizarea sistemelor utilizate pentru Prelucrarea de Date Operator în fața pericolelor provenite din rețele publice prin implementarea unor măsuri fizice și logice împotriva accesului neautorizat. Măsurile de protecție logice trebuie să includă controale ale fluxurilor de informații între sistemele IT interne și rețelele publice externe, precum și ale acțiunile inițiate în rețelele publice și în sistemele utilizate pentru Prelucrarea de Date Operator; și

(ii) Protejarea criptografică a datelor utilizate în scopuri de autentificare care sunt transferate în rețele publice.

1.6 A se asigura că datele personale sunt prelucrate numai în conformitate cu instrucțiunile operatorului, inclusiv prin:

1.6.1 Implementarea și aplicarea unei politici de păstrare a documentelor si respectiv a datelor;

1.6.2 Implementarea și aplicarea politicilor privind accesul, utilizarea și divulgarea datelor cu caracter personal;

1.6.3 Implementarea politicilor de confidențialitate, inclusiv a politicilor de securitate privind protecția datelor și a instrucțiunilor de gestionare a sistemelor informatice în conformitate cu legea;

1.6.4 Cooperarea cu Operatorul în cea mai mare măsură rezonabilă, inclusiv prin răspunsul la întrebările acesteia, informarea acesteia cu privire la inspecțiile efectuate de o autoritate competenta in domeniul prelucrării datelor cu caracter personal și adoptarea cererilor de respectare a legii; și

1.6.5 Numirea unui ofițer de securitate informatică/protecție a datelor, în cazul în care acest lucru este impus de lege sau devine in mod rezonabil necesar, care va fi responsabil pentru respectarea principiilor de securitate/protecție a datelor prevăzute de lege si/sau cerute de Operator si/sau prin APD. Furnizorul de Servicii va furniza companiei Operatorului datele de contact ale unui asemenea ofițer.

1.7 A se asigura că Datele cu Caracter Personal Operator sunt protejate împotriva distrugerii sau pierderii accidentale, inclusiv prin:

1.7.1 Proceduri de realizare de copii de rezervă (de exemplu, sisteme automate de realizare a unor copii de rezervă online și pe suport fizic);

1.7.2 Stocarea copiilor de rezervă în locuri securizate (în încăperi distincte de cele în care se află originale), împotriva furtului, preluării, accesarii, modificării, deteriorării sau distrugerii neautorizate (și șterse imediat după ce acestea nu mai sunt necesare);

1.7.3 Surse de alimentare de rezervă pentru infrastructura critică;

1.7.4 Sisteme de protecție împotriva virușilor pentru protecția stațiilor de lucru și a serverelor;

Pentru menținerea securității prelucrării datelor cu caracter personal (în special împotriva virușilor informatici) Furnizorul de Servicii va lua măsuri care vor consta în:

a) interzicerea folosirii de către persoanele autorizate a programelor software care provin din surse externe sau dubioase;

b) informarea periodica a persoanelor autorizate în privința pericolului privind virușii informatici;

c) implementarea unor sisteme automate de devirusare și de securitate a sistemelor informatice;

d) dezactivarea, pe cât posibil, a tastei "Print screen", atunci când sunt afișate pe monitor date cu caracter personal, interzicându-se astfel scoaterea la imprimantă a acestora.

1.7.5 Asigurarea integrității, disponibilității și rezistenței continue ale sistemelor și serviciilor sale de prelucrare;

1.7.6 Reguli firewall, revizuite periodic de personalul IT;

1.7.7 Păstrarea echipamentelor informatice sensibile în zone securizate; și

1.7.8 Planurile de urgență pentru recuperarea de pe urma situațiilor de dezastru, inclusiv cele cauzate de întreruperi de curent sau de interferențe cu rețelele electrice.