GYMBOLAND S.R.L.

REGULAMENTUL
privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date

Intrat în vigoare pe data de 30 august 2018

Capitolul I. Datele de identificare ale operatorului

Art. 1. Denumirea operatorului. (1) Operatorul de date cu caracter personal este GYMBOLAND S.R.L..

Sediul social: București, Bd. Iuliu Maniu, nr. 7, sectorul 6.
Număr de ordine în Registrul Comerțului: J40/8102/2008 atribuit pe data de 09.05.2008.
Identificator unic la nivel european (EUID): ROONRC.J40/8102/2008.
Cod unic de înregistrare: 23848930.
Forma de organizare: societate cu răspundere limitată pe acțiuni (S.R.L.).
Durata de funcționare: nelimitată.
Certificat de înregistrare: B2736760 emis pe data de 02.04.2013.
Actul de înmatriculare și autorizare: încheierea judecătorească nr. 8000/09.05.2008.
Starea societății la data întocmirii raportului: în funcțiune.

Art. 2. Activitatea principală a operatorului. (1) Alte activități recreative și distractive n.c.a – cod CAEN 9329 conform codificării prevăzute de *Ordinul nr. 337/2007 privind actualizarea Clasificării activităților din economia națională (CAEN) emis de Președintele Institutului Național de Statistică.*

(2) Conform declarației nr. 14567/15.01.2013 operatorul desfășoară activități proprii de birou la sediul social din București, Bd. Iuliu Maniu, nr. 7, corp A, camera B30, etajul 4, sectorul 6.

(3) Număr mediu de salariați pentru anul 2018: 30 de salariați, conform datelor cuprinse în furnizarea de informații emisă de Oficiul Registrului Comerțului București cu nr. 1446845/29.08.2018.

Capitolul II. Scopul și domeniul de aplicare al Regulamentului

Art. 3. Regulamentul urmărește asigurarea efectuării prelucrării datelor cu caracter personal în cadrul activităților desfășurate de operatorul de date cu caracter personal GYMBOLAND S.R.L în conformitate cu *Regulamentul UE nr. 679/2016 al Parlamentului European și al Consiliului din data de 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE,* denumit în continuare Regulamentul UE nr. 679/2016.

Art. 4. Scopul Regulamentului este de a garanta și proteja drepturile și libertățile fundamentale ale persoanelor fizice, în special a dreptului la viață intimă, familială și privată, cu privire la prelucrarea datelor cu caracter personal.

Art. 5. Regulamentul se aplică prelucrărilor de date cu caracter personal, efectuate, în tot sau în parte, prin mijloace automate, precum și prelucrării prin alte mijloace decât cele automate a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau care sunt destinate să fie incluse într-un asemenea sistem.

Art. 6. Regulamentul urmărește aplicarea dispozițiilor legale referitoare la protecția datelor cu caracter personal prin:

a) înțelegerea contextului adoptării Regulamentului UE nr. 679/2016 și cunoașterea domeniului de aplicare;
b) însușirea definițiilor de bază prevăzute în Regulamentul UE nr. 679/2016, respectiv a noțiunilor de date cu caracter personal, categorii de date cu caracter personal, operator de date cu caracter personal, subiect al protecției datelor cu caracter personal, protecția datelor cu caracter personal, încălcarea securității datelor cu caracter personal;
c) cunoașterea principiilor prelucrării datelor cu caracter personal;
d) identificarea obligațiilor operatorului de date cu caracter personal;
e) identificarea drepturilor subiectului protecției datelor cu caracter personal;
f) identificarea tipurilor de prelucrări de date cu caracter personal;
g) identificarea categoriilor de date cu caracter personal prelucrate;
h) identificarea temeiului legal în baza căruia se efectuează prelucrarea raport la art. 6 din Regulamentul UE nr. 679/2016;
i) identificarea persoanelor care prelucrează datele cu caracter personal;
j) asigurarea că persoanele împuternicite își cunosc obligațiile și responsabilitățile;
k) identificarea fluxului de date, cu indicarea originii și a destinației datelor, în special pentru a identifica eventualele transferuri de date în afara Uniunii Europene;
l) verificarea existenței și clauzelor contractuale și actualizarea obligațiilor persoanelor împuternicite privind securitatea, confidențialitatea și protecția datelor cu caracter personal prelucrate;
m) identificarea eventualelor prelucrări de date cu caracter personal susceptibile de a prezenta riscuri ridicate pentru drepturile și libertățile persoanelor fizice pentru a determina dacă operatorul ca efectua o evaluare a impactului asupra protecției datelor în condițiile art. 35 din Regulamentul UE nr. 679/2016;
n) identificarea eventualelor prelucrări de date cu caracter personal susceptibile de a impune desemnarea responsabilului cu protecția datelor, persoană care să exercite o misiune de informare, de consiliere și de control în plan intern, în condițiile art. 37-39 din Regulamentul UE nr. 679/2016;
o) stabilirea măsurilor tehnice și organizatorice pentru protejarea datelor;
p) elaborarea procedurilor interne pentru a asigura permanent un nivel ridicat de protecție a datelor cu caracter personal.

Art. 7. Aplicarea corectă a prezentului regulament va fi monitorizată de operator. Nerespectarea intenționată sau din culpă a dispozițiilor regulamentului poate conduce la pierderi financiare și reputaționale semnificative pentru operator, și, posibil, la consecințe disciplinare pentru angajații operatorului responsabili

Capitolul III. Contextul adoptării Regulamentului UE nr. 679/2016 și cunoașterea domeniului de aplicare

Art. 8. (1) Parlamentul European și Consiliul au adoptat, în data de 27 aprilie 2016, Regulamentul UE nr. 679/2016, fiind publicat în Jurnalul Oficial al Uniunii L119 din data de 4 mai 2016. Prevederile lui sunt direct aplicabile în toate statele membre din data de 25 mai 2018.

(2) Regulamentul UE nr. 679/2016 impune un set unic de reguli în materia protecției datelor cu caracter personal, înlocuind Directiva 95/46/CE și, implicit, prevederile *Legii nr. 677/2001 pentru*

protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

Art. 9. Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal este un drept fundamental. Articolul 8 alineatul (1) din Carta drepturilor fundamentale a Uniunii Europene („carta") și articolul 16 alineatul (1) din Tratatul privind funcționarea Uniunii Europene (TFUE) prevăd dreptul oricărei persoane la protecția datelor cu caracter personal care o privesc.

Art. 10. (1) Principiile și normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal, indiferent de cetățenia sau de locul de reședință al persoanelor fizice, trebuie să fie cât mai bine înțelese și aplicate, astfel încât să respecte drepturile și libertățile fundamentale persoanelor fizice, în special dreptul la protecția datelor cu caracter personal.

(2) Protecția conferită de Regulamentul UE nr. 679/2016 vizează persoanele fizice, indiferent de cetățenia sau de locul de reședință al acestora, în ceea ce privește prelucrarea datelor cu caracter personal ale acestora.

(3) Regulamentul UE nr. 679/2016 nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice.

Art. 11. Dreptul la protecția datelor cu caracter personal nu este un drept absolut; acesta trebuie luat în considerare în raport cu funcția pe care o îndeplinește în societate și echilibrat cu alte drepturi fundamentale, în conformitate cu principiul proporționalității. Regulamentul UE 679/2016 respectă toate drepturile fundamentale și libertățile și principiile recunoscute în cartă astfel cum sunt consacrate în tratate, în special respectarea vieții private și de familie, a reședinței și a comunicațiilor, a protecției datelor cu caracter personal, a libertății de gândire, de conștiință și de religie, a libertății de exprimare și de informare, a libertății de a desfășura o activitate comercială, dreptul la o cale de atac eficientă și la un proces echitabil, precum și diversitatea culturală, religioasă și lingvistică.

Art. 12. Evoluțiile tehnologice rapide și globalizarea au generat noi provocări pentru protecția datelor cu caracter personal. Amploarea colectării și a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite atât societăților private, cât și autorităților publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităților lor. Din ce în ce mai mult, persoanele fizice fac publice la nivel mondial informații cu caracter personal. Tehnologia a transformat deopotrivă economia și viața socială și ar trebui să faciliteze în continuare libera circulație a datelor cu caracter personal în cadrul Uniunii și transferul către țări terțe și organizații internaționale, asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal.

Art. 13. Pentru buna funcționare a pieței interne este necesar ca libera circulație a datelor cu caracter personal în cadrul Uniunii să nu fie restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal. Așadar, libera circulație a datelor cu caracter personal în interiorul Uniunii nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

Art. 14. Regulamentul UE nr. 679/2016 se aplică:

a) prelucrării datelor cu caracter personal în cadrul activităților derulate la sediul unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii;
b) prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de (i) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată, sau (ii) monitorizarea comportamentului dacă acesta se manifestă în cadrul Uniunii;
c) prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internațional public.

Capitolul IV. Definiții

Art. 15. În sensul Regulamentului UE nr. 679/2016 :

1. „date cu caracter personal” înseamnă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;
2. „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;
3. „restricționarea prelucrării” înseamnă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;
4. „creare de profiluri” înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;
5. „pseudonimizare” înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;
6. „sistem de evidență a datelor” înseamnă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;
7. „operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii

sau în dreptul intern;

8. „persoană împuternicită de operator” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;
9. „destinatar” înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia (căruia) îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu dreptul Uniunii sau cu dreptul intern nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;
10. „parte terță” înseamnă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;
11. „consimțământ” al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;
12. „încălcarea securității datelor cu caracter personal” înseamnă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;
13. „date genetice” înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;
14. „date biometrice” înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;
15. „date privind sănătatea” înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;
16. „sediu principal” înseamnă:
    (a) în cazul unui operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acestuia în Uniune, cu excepția cazului în care deciziile privind scopurile și mijloacele de prelucrare a datelor cu caracter personal se iau într-un alt sediu al operatorului din Uniune, sediu care are competența de a dispune punerea în aplicare a acestor decizii, caz în care sediul care a luat deciziile respective este considerat a fi sediul principal;
    (b) în cazul unei persoane împuternicite de operator cu sedii în cel puțin două state membre, locul în care se află administrația centrală a acesteia în Uniune, sau, în cazul în care persoana împuternicită de operator nu are o administrație centrală în Uniune, sediul din Uniune al persoanei împuternicite de operator în care au loc activitățile principale de prelucrare, în contextul activităților unui sediu al persoanei împuternicite de operator, în măsura în care aceasta este supusă unor obligații specifice în temeiul prezentului regulament;

17. „reprezentant” înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27 din Regulamentul UE nr. 679/2016, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul prezentului regulament;
18. „întreprindere” înseamnă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfășoară în mod regulat o activitate economică;
19. „grup de întreprinderi” înseamnă o întreprindere care exercită controlul și întreprinderile controlate de aceasta;
20. „reguli corporatiste obligatorii” înseamnă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări terțe în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;
21. „autoritate de supraveghere” înseamnă o autoritate publică independentă instituită de un stat membru în temeiul articolului 51 din Regulamentul UE nr. 679/2016;
22. „autoritate de supraveghere vizată” înseamnă o autoritate de supraveghere care este vizată de procesul de prelucrare a datelor cu caracter personal deoarece:
    (a) operatorul sau persoana împuternicită de operator este stabilită pe teritoriul statului membru al autorității de supraveghere respective;
    (b) persoanele vizate care își au reședința în statul membru în care se află autoritatea de supraveghere respectivă sunt afectate în mod semnificativ sau sunt susceptibile de a fi afectate în mod semnificativ de prelucrare; sau
    (c) la autoritatea de supraveghere respectivă a fost depusă o plângere;
23. „prelucrare transfrontalieră” înseamnă:
    (a) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților sediilor din mai multe state membre ale unui operator sau ale unei persoane împuternicite de operator pe teritoriul Uniunii, dacă operatorul sau persoana împuternicită de operator are sedii în cel puțin două state membre; sau
    (b) fie prelucrarea datelor cu caracter personal care are loc în contextul activităților unui singur sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, dar care afectează în mod semnificativ sau este susceptibilă de a afecta în mod semnificativ persoane vizate din cel puțin două state membre;
24. „obiecție relevantă și motivată” înseamnă o obiecție la un proiect de decizie în scopul de a stabili dacă există o încălcare a prezentului regulament sau dacă măsurile preconizate în ceea ce privește operatorul sau persoana împuternicită de operator respectă prezentul regulament, care demonstrează în mod clar importanța riscurilor pe care le prezintă proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, libera circulație a datelor cu caracter personal în cadrul Uniunii;
25. „serviciile societății informaționale” înseamnă un serviciu astfel cum este definit la articolul 1 alineatul (1) litera (b) din Directiva 98/34/CE a Parlamentului European și a Consiliului;

26. „organizație internațională” înseamnă o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord.

Art. 16. Alți termeni

a) **persoana vizată** - persoana fizică ale cărei date cu caracter personal sunt prelucrate:
i) date personale ale clienților persoane fizice;
ii) date personale ale partenerilor persoane fizice;
iii) date personale ale persoanelor fizice care au calitatea de reprezentanți legali sau convenționali ai clienților sau partenerilor persoane juridice;
iii) administratorii, directorii, mandatarii ori salariații operatorului;
b) **a colecta** - a strânge, a aduna, a primi date cu caracter personal de la persoanele prevăzute la lit. a);
c) **a dezvălui** - a transmite, a disemina, a face disponibile în orice alt mod date cu caracter personal, în afara operatorului;
d) **a utiliza** - a se folosi datele cu caracter personal de către și în interiorul operatorului;
e) **nivel de protecție și de securitate adecvat al prelucrărilor de date cu caracter personal** - nivelul de securitate proporțional riscului, pe care îl comportă prelucrarea față de datele cu caracter personal respective și față de drepturile și libertățile persoanelor și conform cerințelor minime de securitate a prelucrărilor de date cu caracter personal, elaborate de autoritatea de supraveghere și actualizate corespunzător stadiului dezvoltării tehnologice și costurilor implementării acestor măsuri.

Capitolul V. Principiile prelucrării datelor cu caracter personal

Art. 17. (1) GYMBOLAND S.R.L. prelucrează datele cu caracter personal respectând principiul transparenței. Orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal sunt ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar.

(2) În virtutea acestui principiu, persoanele vizate sunt informate cu privire la identitatea operatorului și scopurile prelucrării, precum și la oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care le privesc care sunt prelucrate.

(3) Persoanele fizice vizate sunt informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea. În special, scopurile specifice în care datele cu caracter personal sunt prelucrate sunt explicite și legitime și determinate la momentul colectării datelor respective.

Art. 18. Datele cu caracter personal sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1) din Regulamentul UE nr. 679/2016 („limitări legate de scop”);

(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”); datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum. Datele cu caracter personal sunt prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace;

(d) exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate”);

(e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1) din Regulamentul UE nr. 679/2016, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor și libertăților persoanei vizate („limitări legate de stocare”);

(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”);

(g) șterse dacă nu mai sunt necesare și dacă termenul de păstrare s-a împlinit. În vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, sunt stabilite de către operator termene pentru ștergere sau revizuirea periodică.

Capitolul VI. Scopurile prelucrării datelor cu caracter personal. Temeiurile legale ale prelucrării

Art. 19. Datele cu caracter personal colectate de operatorul GYMBOLAND S.R.L. sunt prelucrate:

a) în scopul etapelor premergătoare încheierii oricăror contracte comerciale la cererea persoanelor vizate;
b) în scopul încheierii/executării/modificării/încetării contractelor comerciale, în special asigurarea serviciilor principale prestate pentru îndeplinirea obiectului de activitate principal al societății, respectiv servicii alte activități recreative și distractive;
c) în scopul îndeplinirii obligațiilor prevăzute în actele normative (obligații legale);
d) în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate; așadar, interesele legitime ale operatorului, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terțe părți, pot constitui un temei juridic pentru prelucrare, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate, luând în considerare așteptările rezonabile ale persoanelor vizate bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. În orice caz, existența unui interes legitim necesită

o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul și în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele și drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanțe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză. Operatorii care fac parte din același grup de întreprinderi sau instituții afiliate societății GYMBOLAND S.R.L. pot avea un interes legitim de a transmite date cu caracter personal în cadrul grupului de întreprinderi în scopuri administrative interne, inclusiv în scopul prelucrării datelor cu caracter personal ale clienților sau angajaților. Principiile generale ale transferului de date cu caracter personal, în cadrul unui grup de întreprinderi, către o întreprindere situată într-o țară terță rămân neschimbate. De asemenea, prelucrarea de date cu caracter personal care are drept scop marketingul direct poate fi considerată ca fiind desfășurată pentru un interes legitim.

e) în scopul etapelor premergătoare încheierii contractelor de individuale de muncă la cererea persoanelor vizate, în scopul recrutării;

f) în scopul încheierii/executării, respectării clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al egalității și diversității la locul de muncă, al asigurării sănătății și securității la locul de muncă, precum și în scopul exercitării și beneficierii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și în scopul încetării/stingerii raporturilor de muncă;

g) în baza consimțământului persoanei vizate. Cu privire la prelucrarea datelor cu caracter personal în temeiul consimțământului se va ține seama de cerințele referitoare la acest temei. Astfel, consimțământul va fi solicitat persoanei vizate printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declarație făcută în scris, inclusiv în format electronic, sau verbal care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu vor constitui consimțământ. Consimțământul va viza toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul va fi dat pentru toate scopurile prelucrării. În cazul în care consimțământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul. Consimțământul nu va fi considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată. În anumite circumstanțe, cum ar conversațiile telefonice, consimțământul poate fi dat verbal. În toate cazurile acordarea consimțământului trebuie să fie documentată. Așadar, fără a aduce atingere dispozițiilor legale care reglementează obligația operatorului de a respecta și de a ocroti viața intimă, familială și privată, **consimțământul** persoanei vizate **nu este cerut** în următoarele cazuri:

- când prelucrarea este necesară în vederea executării unui contract sau antecontract la care persoana vizată este parte ori în vederea luării unor măsuri, la cererea acesteia, înaintea încheierii unui contract sau antecontract;

- când prelucrarea este necesară în vederea protejării vieții, integrității fizice sau sănătății persoanei vizate ori a unei alte persoane amenințate;
- când prelucrarea este necesară în vederea îndeplinirii unei obligații legale a operatorului;
- când prelucrarea este necesară în vederea aducerii la îndeplinire a unor măsuri de interes public sau care vizează exercitarea prerogativelor de autoritate publică cu care este învestit operatorul sau terțul căruia îi sunt dezvăluite datele;
- când prelucrarea este necesară în vederea realizării unui interes legitim al operatorului sau al terțului căruia îi sunt dezvăluite datele, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate;
- când prelucrarea privește date obținute din documente accesibile publicului, conform legii;
- când prelucrarea este făcută exclusiv în scopuri statistice, de cercetare istorică sau științifică, iar datele rămân anonime pe toată durata prelucrării.

Art. 20. (1) Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele cu caracter personal au fost inițial colectate este permisă doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele cu caracter personal au fost inițial colectate.

(2) Temeiul juridic prevăzut în dreptul Uniunii sau în dreptul intern pentru prelucrarea datelor cu caracter personal poate constitui, de asemenea, un temei juridic pentru prelucrarea ulterioară.

(3) Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate inițial datele cu caracter personal, operatorul, după ce a îndeplinit toate cerințele privind legalitatea prelucrării inițiale, va ține seama, printre altele, de orice legătură între respectivele scopuri și scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de așteptările rezonabile ale persoanelor vizate, bazate pe relația lor cu operatorul, în ceea ce privește utilizarea ulterioară a datelor, de natura datelor cu caracter personal, de consecințele prelucrării ulterioare preconizate asupra persoanelor vizate, precum și de existența garanțiilor corespunzătoare atât în cadrul operațiunilor de prelucrare inițiale, cât și în cadrul operațiunilor de prelucrare ulterioare preconizate.

Capitolul VII. Reguli speciale privind prelucrarea datelor cu caracter personal

Art. 21. (1) Prelucrarea datelor cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, filozofice sau de natură similară, de apartenența sindicală, precum și a datelor cu caracter personal privind starea de sănătate sau viața sexuală este interzisă.

(2) Prevederile alin. (1) nu se aplică în următoarele cazuri:

a) când persoana vizată și-a dat în mod expres consimțământul pentru o astfel de prelucrare, cu excepția cazului în care dreptul Uniunii Europene sau dreptul intern prevede ca interdicția prevăzută la alineatul (1) să nu poată din ridicată prin consimțământul persoanei vizate;

b) când prelucrarea este necesară în scopul respectării obligațiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, al securității și protecției sociale, cu respectarea garanțiilor prevăzute de lege; o eventuală dezvăluire către un terț a datelor prelucrate poate fi efectuată numai dacă există o obligație legală a operatorului în acest sens sau dacă persoana vizată a consimțit expres la această dezvăluire;

c) când prelucrarea este necesară pentru protecția vieții, integrității fizice sau a sănătății persoanei vizate ori a altei persoane, în cazul în care persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;

d) când prelucrarea este efectuată în cadrul activităților sale legitime de către o fundație, asociație sau de către orice altă organizație cu scop nelucrativ și cu specific politic, filozofic, religios ori sindical, cu condiția ca persoana vizată să fie membră a acestei organizații sau să întrețină cu aceasta, în mod regulat, relații care privesc specificul activității organizației și ca datele să nu fie dezvăluite unor terți fără consimțământul persoanei vizate;

e) când prelucrarea se referă la date făcute publice în mod manifest de către persoana vizată;

f) când prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiție;

g) când prelucrarea este necesară în scopuri de medicină preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente medicale pentru persoana vizată ori de gestionare a serviciilor de sănătate care acționează în interesul persoanei vizate, cu condiția ca prelucrarea datelor respective să fie efectuate de către ori sub supravegherea unui cadru medical supus secretului profesional sau de către ori sub supravegherea unei alte persoane supuse unei obligații echivalente în ceea ce privește secretul;

h) când legea prevede în mod expres aceasta în scopul protejării unui interes public important/major, cu condiția ca prelucrarea să se efectueze cu respectarea drepturilor persoanei vizate și a celorlalte garanții prevăzute legale.

(3) Prevederile alin. (2) nu aduc atingere dispozițiilor legale care reglementează obligația autorităților publice de a respecta și de a ocroti viața intimă, familială și privată.

Art. 22. Prelucrarea datelor cu caracter personal referitoare la săvârșirea de infracțiuni de către persoana vizată ori la condamnări penale, măsuri de siguranță sau sancțiuni administrative ori contravenționale, aplicate persoanei vizate, poate fi efectuată numai de către sau sub controlul autorităților publice, în limitele puterilor ce le sunt conferite prin lege și în condițiile stabilite de legile speciale care reglementează aceste materii. Orice registru cuprinzător al condamnărilor penale se ține numai sun controlul unei autorități de stat.

Capitolul VIII. Categorii de date cu caracter personal prelucrate

Art. 23. (1) GYMBOLAND S.R.L. prelucrează următoarele date cu caracter personal:

a) Date despre clienți, inclusiv numele, prenumele și data nașterii copilului clientului care solicită serviciile operatorului, parteneri comerciali și reprezentanți ai acestora. Prelucrarea datelor pentru o relație contractuală

Datele personale ale eventualilor clienți, clienți existenți și parteneri, precum și ale persoanelor fizice ce îi reprezintă, pot fi procesate în scopul încheierii, executării și finalizării unui contract. Datele cu caracter personal sunt prelucrate și în cursul negocierilor precontractuale, spre exemplu pentru a pregăti oferte sau ale documente în scopul încheierii contractului. Persoanele vizate pot fi contactate în timpul negocierilor/procesului de pregătire a contractului folosind informațiile persoanele pe care acestea lea-u furnizat. Orice restricții solicitate de persoanele vizate în timpul negocierilor trebuie respectate. De regulă, sunt prelucrate următoarele categorii de date cu caracter personal: i) numele și prenumele (ii) data nașterii (iii) locul nașterii (iii) domiciliul (iii) seria și numărul cărții de identitate (iv) codul numeric personal (v) numărul de telefon (v) e-mail (vi) informații și date legate de pregătirea educațională și profesională (vii) informații și date legate de profesia și funcția exercitată (viii) numele, prenumele și data nașterii copilului pentru care se solicită serviciile operatorului.

b) Datele persoanelor care solicită încheierea unui contract individual de muncă

Operatorul prelucrează (i) numele și prenumele (ii) data nașterii (iii) locul nașterii (iii) domiciliul (iii) seria și numărul cărții de identitate (iv) codul numeric personal (v) numărul de telefon (v) e-mail (vi) informații și date legate de pregătirea educațională și profesională (vii) informații și date legate de profesiile și funcțiile exercitate. În situația în care candidatul este respins, datele sale trebuie să fi șterse, în conformitate cu termenul de păstrare necesar, cu excepția cazului în care candidatul a fost de acord ca datele sale să rămână la dosar pentru un viitor proces de selecție. De asemenea, este necesar să se obțină consimțământul pentru a prelucra datele în cadrul altor companii din grup. Dacă în timpul procedurii de aplicare este necesară colectarea informațiilor despre un candidat de la terță parte, se vor respecta, de asemenea, cerințele legale corespunzătoare.

c) Datele salariaților sau ale persoanelor asimilate salariaților (administratori, manageri, directori, etc)

Operatorul prelucrează (i) numele și prenumele (ii) data nașterii (iii) locul nașterii (iii) domiciliul (iii) seria și numărul cărții de identitate (iv) codul numeric personal (v) numărul de telefon (v) e-mail (vi) informații și date legate de pregătirea educațională și profesională (vii) informații și date legate de profesiile și funcțiile exercitate.

(2) GYMBOLAND S.R.L. nu prelucrează datele cu caracter personal ale copiilor pentru crearea de profiluri de personalitate sau de utilizator.

Capitolul IX. Drepturile persoanelor vizate

Art. 24. În virtutea art. 12 din Regulamentul UE 679/2016 privind transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanelor vizate, operatorul va lua măsuri adecvate pentru a furniza persoanei vizate orice informații legate de drepturile persoanelor vizate. În acest sens, operatorul va adopta *Procedura privind exercitarea drepturilor persoanelor vizate* pentru garantarea următoarelor drepturi:

Dreptul de a fi informat. Persoana vizată are dreptul de a primi informații clare, transparente, ușor de înțeles și ușor accesibile cu privire la modul în care sunt prelucrate datele sale, inclusiv detalii privind drepturile sale, în calitate de persoană vizată.

Dreptul de acces la date. Persoana vizată are dreptul de a accesa datele prelucrate despre ea, fără a percepe vreun fel de taxă la primele furnizări de date.

Dreptul la rectificarea datelor. În cazul în care persoana vizată identifică că datele sale sunt prelucrate incorecte, incomplet sau inexacte poate solicita rectificarea acestora.

Dreptul de ștergere a datelor (*dreptul de a fi uitat*). Persoana vizată are dreptul de a solicita ștergerea datelor tale în situațiile prevăzute în *Procedura privind exercitarea drepturilor persoanelor vizate*

Dreptul de a restricționa prelucrarea. Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării datelor în oricare dintre situațiile *Procedura privind exercitarea drepturilor persoanelor vizate*.

Dreptul de a se opune marketing-ului direct (inclusiv profilarea în scop de marketing direct). Persoana vizată se poate opune oricând și dezabona la comunicările de marketing direct în orice moment.

Dreptul de a se opune prelucrării bazate pe interes legitim. Persoana vizată se poate opune în orice moment oricărei prelucrări de date atunci când la o astfel de prelucrare se bazează pe interesul legitim al operatorului.

Dreptul de portabilitate. Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazurile prevăzute de art. 20 alin. (1) din Regulamentul UE nr. 679/2016.

Dreptul de a face plângeri la autoritatea de supraveghere. Persoana vizată are dreptul să depună orice plângeri în fața Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal („A.N.S.P.D.C.P.”) asupra modului în care îi sunt prelucrate datele tale personale.

Capitolul X. Obligațiile operatorului

Art. 25. În virtutea principiului responsabilității prelucrării datelor cu caracter personal, GYMBOLAND S.R.L:

a) urmărește cu prioritate conformarea cu cerințele Regulamentului UE nr. 679/2016;
b) promovează o cultură organizațională care respectă dreptul la viață privată al persoanelor vizate;
c) gestionează responsabil datele cu caracter personal;
d) prelucrează datele cu caracter personal în mod legal, transparent și echitabil;
e) va identifica eventualele prelucrări de date cu caracter personal susceptibile de a prezenta riscuri ridicate pentru drepturile și libertățile persoanelor fizice pentru a determina dacă se impune evaluarea impactului asupra protecției datelor;
f) desemna responsabilul cu protecția datelor dacă va aprecia ca sunt întrunite cerințele art. 37 din Regulamentul UE nr. 679/2016;
g) creează mecanisme de raportare a conformității.

Art. 26. Orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite, inclusiv persoana împuternicită, care are acces la date cu caracter personal, nu poate să le prelucreze decât pe baza instrucțiunilor operatorului, cu excepția cazului în care acționează în temeiul unei obligații legale.

Art. 27. (1) Datele persoanele sunt considerate confidențiale.
(2) Orice prelucrare neautorizată a acestor date de către salariați este interzisă. Orice procesare de date efectuată de un salariat care nu a fost autorizat să o îndeplinească, ca parte a atribuțiilor sale de serviciu, este neautorizată.

(3) Salariații pot avea acces la date persoane numai pentru scopul sarcinii de serviciu. Acest lucru necesită punerea în aplicare a rolurilor și responsabilităților fiecărui salariat. Este interzisă prelucrarea datelor cu caracter personal în scopuri private sau comerciale, dezvăluirea făcută persoanelor neautorizate sau punerea la dispoziție a datelor către persoane neautorizate în orice mod. Șefii de departamente și departamentul de resurse umane vor informa salariații la începutul relației de muncă cu privire la obligația de a proteja confidențialitate datelor personale. Această obligație produce efecte și după încetarea contractului individual de muncă.

(4) Operatorul este obligat să aplice măsurile tehnice și organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat, în special dacă prelucrarea respectivă comportă transmisii de date în cadrul unei rețele, precum și împotriva oricărei alte forme de prelucrare ilegală.

(5) Aceste măsuri trebuie să asigure, potrivit stadiului tehnicii utilizate în procesul de prelucrare și de costuri, un nivel de securitate adecvat în ceea ce privește riscurile pe care le reprezintă prelucrarea, precum și în ceea ce privește natura datelor care trebuie protejate. Cerințele minime de securitate a datelor cu caracter personal fac parte din managementul securității informațiilor companiei și vor fi actualizate periodic, corespunzător progresului tehnic și experienței acumulate.

(6) Efectuarea prelucrărilor prin persoane împuternicite trebuie să se desfășoare în baza unui contract încheiat în formă scrisă, care va cuprinde în mod obligatoriu:

a) obligația persoanei împuternicite de a acționa doar în baza instrucțiunilor primite de la operator;

b) faptul că îndeplinirea obligațiilor prevăzute în prezentul articol revine și persoanei împuternicite.

Art. 28. În măsura în care vor fi incidente dispozițiile art. 30 din Regulamentul UE nr. 679/2016 privind evidențele activităților de prelucrare, operatorul va întocmi și păstra evidențe ale activităților de prelucrare aflate în responsabilitatea sa. Operatorul cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor lor, și va pune la dispoziția acesteia, la cerere, aceste evidențe, pentru a putea fi utilizate în scopul verificării operațiunilor de prelucrare respective.

Art. 29. În măsura în care vor fi incidente dispozițiile art. 37 din Regulamentul UE nr. 679/2016 privind desemnarea operatorului de date cu caracter personal, operatorul va desemna responsabilul cu protecția datelor ținând seama și de prevederile art. 38 și 39 din Regulamentul UE nr. 679/2016.

Art. 30. În măsura în care vor fi incidente dispozițiile art. 35 din Regulamentul UE nr. 679/2016 privind evaluarea impactului asupra protecției datelor, operatorul va întocmi evaluarea anterior prelucrării datelor solicitând avizul responsabilului cu protecția datelor dacă acesta a fost desemnat.

Capitolul XI. Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal

Art. 31. (1) Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret

profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

(2) De îndată ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul va notifica încălcarea autorității de supraveghere, fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore după ce a luat la cunoștință de existența acesteia, cu excepția cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta va cuprinde motivele întârzierii, iar informațiile pot fi furnizate treptat, fără altă întârziere.

(3) Operatorul va comunica persoanei vizate încălcarea securității datelor cu caracter personal, fără întârzieri nejustificate, atunci când încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanei fizice, pentru a-i permite să ia măsurile de precauție necesare. Comunicarea trebuie să descrie într-un limbaj clar și simplu natura încălcării securității datelor cu caracter personal și să cuprindă datele de contact ale responsabilului cu protecția datelor sau alt punct de contact de unde se pot obține mai multe informații, consecințele probabile ale încălcării securității datelor cu caracter persona, precum și recomandările pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative.

(4) Comunicările către persoanele vizate vor fi efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu autoritatea de supraveghere, respectându-se orientările furnizate de aceasta sau de alte autorități competente, cum ar fi autoritățile de aplicare a legii. De exemplu, necesitatea de a atenua un risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine către persoanele vizate, în timp ce necesitatea de a implementa măsuri corespunzătoare împotriva încălcării în continuare a securității datelor cu caracter personal sau împotriva unor încălcări similare ale securității datelor cu caracter personal ar putea justifica un termen mai îndelungat pentru comunicare.

(5) Informarea persoanei vizate nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

a) operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

b) operatorul a luată măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate nu mai este susceptibil să se realizeze;

c) ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sa se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

Capitolul XII. Transferurile de date cu caracter personal

Art. 32. (1) Fluxurile de date cu caracter personal către și dinspre țări situate în afara Uniunii Europene (state terțe) și organizații internaționale pot fi necesare pentru dezvoltarea activităților desfășurate de operator, aria sa de activitate fiind comerțul. Operatorul este informat că în cazul în care se transferă date cu caracter personal din Uniunea Europeană către operatori, persoane împuternicite de operatori sau alți destinatari din țări terțe sau organizații internaționale, nivelul de protecție a persoanelor fizice asigurat în Uniune nu ar trebui să fie diminuat. În acest sens, un transfer va avea loc numai dacă, sub rezerva respectării celorlalte dispoziții ale Regulamentului UE nr. 679/2006, operatorul sau persoana

împuternicită de operator îndeplinește condițiile prevăzute de dispozițiile Regulamentului UE nr. 679/2006 privind transferul de date cu caracter personal către țări terțe sau organizații internaționale.

(2) Transferul de date cu caracter personal în afara spațiului Uniunii Europene poate avea loc numai dacă în următoarele situații:

a) Comisia Europeană a emis decizie de adecvare în baza căreia s-a constatat că țara terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară sau organizația internațională în cauză asigură un nivel de protecție adecvat. Transferurile realizate în aceste condiții nu necesită autorizări speciale. Lista țărilor care îndeplinesc la data prezentului Regulament cerințele de adecvare ale Comisiei este publicată în Jurnalul Oficial al Uniunii Europene: http://ec.europa.eu/justice/dataprotection/internațional-transfers/adequacy/index_en.htm;

b) în lipsa unei decizii de adecvare, transferul datelor cu caracter personal într-o țară terță sau într-o organizație internațională poate avea loc numai în una dintre următoarele condiții:

- persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate;

- transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;

- transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;

- transferul este necesar din considerente importante de interes public;

- transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;

- transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau a alte persoana, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul.

Capitolul XIII. Dispoziții finale

Art. 33. Garantul respectării dreptului la protecția datelor cu caracter personal **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)**, cu sediul în București bd. G-ral Gheorghe Magheru, nr.28-30, Sector 1.

Art. 34. Dispozițiile prezentului Regulament se completează cu prevederile Regulamentului UE nr. 679/2016 și cu cele ale *Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).*

Art. 35. Anexele nr. 1- 6 fac parte din prezentul Regulament și conțin:

1) Recomandările organizatorice și tehnice pentru îndeplinirea obligațiilor referitoare la asigurarea confidențialității datelor și informațiilor, pentru păstrarea acestora în siguranță și pentru securitatea și controlul sistemelor informatice;
2) Angajamentul de confidențialitate al salariaților;
3) modelul Declarației de consimțământ pentru prelucrarea datelor;
4) modelul Informării privind utilizarea televiziunii video cu circuit închis (CCTV);

5) modelul de Act adițional privind activitățile de prelucrare a datelor cu caracter personal ale operatorului;
6) modelul de Notificare a Autorității de Supraveghere în cazul unui incident de securitate a datelor.

Art. 36. În virtutea art. 12 din Regulamentul UE 679/2016 privind transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanelor vizate, GYMBOLAND S.R.L. ia măsuri adecvate pentru a furniza persoanei vizate orice informații legate de drepturile persoanelor vizate conform *Procedurii privind exercitarea drepturilor persoanelor vizate.*

Art. 37. Prezentul Regulament împreună cu anexele a fost adoptat de operatorul **GYMBOLAND S.R.L.** la data de 30 august 2018 și intră în vigoare începând cu această dată.

GYMBOLAND
reprezentată de administrator _____

Anexa nr. 1
Recomandări organizatorice și tehnice pentru aplicarea Regulamentului

Recomandări organizatorice

(1) Prelucrarea datelor cu caracter personal va fi permis numai angajaților operatorului în vederea îndeplinirii obligaților de serviciu și persoanelor autorizate în mod expres de operator.

(2) Salariații operatorului vor fi instruiți cu privire la obligațiile ce le incumbă potrivit Regulamentului UE nr. 679/2016 atunci când prelucrează date cu caracter personal în vederea asigurării integrității și confidențialității datelor cu caracter personal.

(3) Accesul persoanelor străine în zonele unde se prelucrează date cu caracter personal se poate face numai după primirea acceptului din partea operatorului prin însoțirea acestora de către un salariat al operatorului.

(4) Accesul personalului ce asigură serviciile de curățenie se va face în baza unui contract cu o entitate autorizată care îndeplinește la rândul ei, condițiile din Regulament. Se va elabora un protocol privind accesul personalului în spațiile de lucru ale operatorului atât în timpul cât și în afara programului de lucru al operatorului.

(5) Crearea unui spațiu de arhivare fizică a actelor care conțin date cu caracter personal ce va respecta cerințele esențiale prevăzute în normativele privind caracteristicele tehnice și funcționale ale spațiilor și echipamentelor de depozitare și conservare a arhivelor. Arhiva va fi încuiată iar accesul va fi permis

numai salariaților operatorului și persoanelor autorizate în mod expres de operator. În vederea identificării spațiului de arhivare și a dotării acestuia se recomandă consultarea unui specialist în domeniul arhivelor.

(6) Pentru evitarea prelucrării necontrolate a datelor operatorul va limita accesul la datele cu caracter personal, va limita prelucrarea la ceea ce este necesar în raport de scopurile în care sunt prelucrate „reducerea la minimum a datelor" și va interzice copierea datelor în afara locurilor în care acestea sunt gestionate.

(7) Tehnica de calcul utilizată în procesul de prelucrare a datelor cu caracter personal va fi amplasată în spații identificate și protejate, accesibile numai salariaților operatorului și persoanelor autorizate în mod expres de operator.

(8) Operatorul și salariații acestuia vor evita:

- divulgarea parolelor/codurilor de securitate care le-au fost alocate în vederea utilizării tehnicii de calcul;
- stocarea parolelor/codurilor de securitate în fișiere necriptate sau programe de gestiune a parolelor în care a fost restricționat accesul, notarea acestora pe hârtie sau în locuri ușor accesibile persoanelor neautorizate;
- înregistrarea parolelor într-un browser fără parolă master;
- utilizarea parolelor având legătură cu utilizatorul (nume, data nașterii, etc);
- păstrarea parolelor presetate;
- trimiterea pe adresa proprie de e-mail a parolelor;
- crearea sau utilizarea de conturi comune mai multor persoane;
- acordarea de drepturi de administrator unor utilizatori care nu dețin drepturi sau cunoștințe de utilizare a tehnicii de calcul;
- omiterea ștergerii conturilor de utilizator ale persoanelor care au părăsit locul de muncă sau care și-au schimbat funcția;
- utilizarea sistemelor de exploatare învechite și neactualizate;
- plasarea bazelor de date pe un server direct accesibil de pe internet;
- păstrarea copiilor de rezervă în același loc cu dispozitivele ce găzduiesc datele întrucât un dezastru major în acel loc va aduce la pierderea definitivă a datelor;
- transmiterea fișierelor ce conțin date cu caracter personal prin intermediul rețelelor de socializare.

(9) Datele cu caracter personal vor putea fi copiate pe suport mobil (memorie externă, stick USB, CD, laptop, tabletă, telefon, etc.) numai în cazurile apreciate ca fiind strict necesare și numai dacă suportul a fost securizat, astfel încât datele pe care le conține să nu poată fi citite/recuperate/copiate/extrase de pe suport, decât cu introducerea unui cod special de securitate.

(10) Tipărirea/fotocopierea datelor cu caracter personal se va realiza numai de salariații operatorului strict în scopul îndeplinirii sarcinilor de serviciu. Accesul la echipamentele ce deservesc aceste operațiuni se va face în baza unui cod alocat fiecărui salariat, ce va permite monitorizarea operațiunilor efectuate.

(11) În caz de utilizare a faxului, instalarea acestuia se va face într-o locație controlată și accesibilă doar de personalul autorizat

(12) Reziduurile în format de hârtie care conțin date cu caracter personal vor fi distruse într-un mod securizat, de exemplu, cu dispozitive de tocat hârtii sau prin angajarea unui specialist în domeniu.

(13) Intervențiile asupra programelor informatice instalate pe echipamentele care prelucrează date cu caracter personal se va face doar cu acordul prealabil al responsabilului desemnat de operator.

(14) Intervențiile asupra echipamentelor hardware ale tehnicii de calcul se va face doar cu acordul prealabil al responsabilului desemnat de operator.

(15) Este interzisă modificarea sau scoaterea din funcțiune a dispozitivelor de securitate ale operatorului.

(16) Spațiile unde se prelucrează datele cu caracter personal vor fi dotate cu alarmă anti-incendiu, detectoare de fum și extinctoare/sisteme automatizate de stingere a incendiilor.

(17) În situația în care este necesar să se intervină asupra instalațiilor existente și a echipamentelor aflate sub tensiune (calculatoare, copiatoare, etc) se recomandă ca aceste intervenții să fie efectuate de persoane autorizate care prestează servicii în baza unor contracte, cu excepția situațiilor de urgență când sunt puse în pericol sănătatea sau viața persoanelor.

(18) La apariția unui incident de securitate salariații operatorului sunt obligați să raporteze de îndată responsabilului cu protecția datelor detaliile cu privire la incident și să respecte instrucțiunile primite de la acesta. Astfel, incidentul va putea fi monitorizat și remediat în cel mai scurt timp. În acest sens, operatorul va desemna persoana responsabilă pentru protecția datelor.

Recomandări tehnice

(19) Tehnica de calcul folosită la prelucrarea datelor cu caracter personal vor fi licențiate și vor avea asigurat suport tehnic din partea producătorului (Microsoft Windows, etc.).

(20) Sistemele IT de prelucrare a datelor vor fi dotate cu sisteme de protecție împotriva riscurilor de securitate provenind din folosirea internetului, sisteme de protecție a rețelei de date, programe antivirus, etc.

(21) Dispozitivele pe care sunt stocate date cu caracter personal vor conține programe pentru criptarea datelor astfel încât în cazul unui furt al dispozitivului sau al datelor, acestea să nu poată fi accesate de către persoanele neautorizate.

(22) Efectuarea periodică de update-uri/upgrade-uri ale sistemelor de operare și ale celorlalte programe utilizate, ale bazelor de date ce stochează informații cu caracter personal, baze de date folosite de sistemul antivirus, programe adiționale, etc.

(23) Configurarea de software-uri pentru ca actualizările de securitate să se realizeze automat, în cel mai scurt timp posibil.

(24) Pentru dispozitivele mobile (laptopuri, telefoane, tablete, etc.) utilizate în cadrul prelucrărilor de date cu caracter personal trebuie asigurată securitatea datelor precum și securitatea fizică a dispozitivelor hardware utilizate.

(25) Pentru protejarea datelor cu caracter personal se vor aplica măsuri de sporire a securității: generare parole complexe, stocarea parolelor în medii sigure, utilizarea cheilor de securitate hardware/software, interzicerea traficului de date cu caracter personal prin rețele de socializare sau în medii de stocare virtuale ce nu oferă garanții de siguranță minimă.

(26) Stațiile de lucru vor fi prevăzute cu un mecanism de blocare automată a sesiunii, în caz de neutilizare a postului pentru o anumită perioadă de timp.

(27) În cazul în care mediile informatice pe care au fost stocate date sunt schimbate ori scoase din uz, se va asigura distrugerea datelor astfel încât acestea să nu poată fi recuperate/accesate.

(28) Efectuarea de către salariații operatorului cu atribuții în administrarea sistemelor IT de cursuri referitoare la Sistemul de Management al Securității Informației (SMSI) în vederea creării unui set de reguli referitoare la managementul riscurilor de securitate a informației. În acest mod, operatorul va dobândi capacitatea de a îndeplini cerințele specificate referitoare la securitatea informației, va putea identifica, analizează și tine sub control riscurile de securitate a informație, indiferent de originea, caracterul și țintele lor.

Operatorul va lua toate măsurile pentru aplicarea efectivă a recomandărilor în scopul conformării cerințelor Regulamentului UE nr. 679/2016 și va urmări aplicarea acestora.

Anexa nr. 2

Angajament de confidențialitate al salariaților

Părți

GYMBOLAND S.R.L., cu sediul social în București, Bd. Iuliu Manciu, nr. 7, sector 6, corp A, etajul 4, camera B30, număr de ordine în Registrul Comerțului: J40/8102/09.05.2008 atribuit pe data de 09.05.2008, identificator unic la nivel european (EUID): ROONRC.J40/8102/2008, cod unic de înregistrare: 23848390, reprezentată de _____ cu funcția de _____ în calitate de **Angajator**
şi

Dl / Dna _____ domiciliat în (localitatea) _____ str._____.nr.,_____ identificat(a) cu actul de identitate seria _____ nr. _____ eliberat de _____în calitate de **Salariat** avînd funcţia de _____ ,

a intervenit prezentul *angajament de confidentialitate*, în scopul păstrării confidenţialităţii datelor, informatiilor şi documentelor, fiind conex contractului individual de muncă încheiat între parti şi înregistrat sub nr._____ din data de _____

Obiect
Obiectul angajamentului de confidențialitate îl reprezintă informațiile pe care le obține Salariatul ca efect al executării contractului de muncă, care sunt strict confidențiale.

Sunt confidențiale următoarele informații:

- datele cu caracter personal ale personalului societății, ale clienților, partenerilor de afaceri și ale reprezentanților acestora;
- situația financiară, licențele și brevetele de invenție;
- proiectele de afaceri;
- produsele și serviciile nelivrate pieței;
- documente care reprezintă poziția de piață a Angajatorului;
- orice alte acte aparținând Angajatorului pe care Salariatul le are la dispoziție

Durata
Salariatul are obligația să păstreze secretul profesional cu privire la actele și faptele despre care a luat cunoștință în cadrul activității sale, chiar și după încetarea raporturilor de muncă, cu excepția cazurilor în care legea sau părțile interesate în eliberează de această obligație.

Răspunderea

Răspunderea juridică a salariatului poate fi angajată în condițiile legii civile pentru încălcarea obligațiilor sale profesionale, atunci când aceasta a cauzat cu vinovăție un prejudiciu angajatorului.

Următoarele situații exonerează de răspundere partea care le invocă:

- informațiile erau cunoscute înainte de a fi obținute de la Angajator;
- informațiile provin dintr-o sură neconfidențială;
- dezvăluirea informației s-a făcut după primire acordului scris pentru aceasta;
- informația era publică la data dezvăluirii ei;

Angajamentul a fost semnat azi _____ _____ în _____ două exemplare, câte unul pentru fiecare parte.

Angajator, Salariat,

Anexa nr. 3

Declarația de consimțământ pentru prelucrarea datelor

Subsemnatul, _____, domiciliat în _____, posesor al _____, CNP _____, sunt de acord ca societatea **GYMBOLAND S.R.L.**, cu sediul social în București, Bd. Iuliu Manciu, nr. 7, sector 6, corp A, etajul 4, camera B30, număr de ordine în Registrul Comerțului: J40/8102/09.05.2008 atribuit pe data de 09.05.2008, identificator unic la nivel european (EUID): ROONRC.J40/8102/2008, cod unic de înregistrare: 23848390, să prelucreze datele mele personale ce sunt colectate în cadrul contractelor de prestări servicii/tranzacțiilor comerciale/în contextul ocupării unui loc de muncă/în executarea contractului de muncă, în următoarele scopuri: furnizarea de informații prin intermediul e-mail-ului, SMS-ului, telefonului, corespondență scrisă, etc. Consimțământul în ceea ce privește prelucrarea datelor cu caracter personal, precum și furnizarea datelor menționate mai jos sunt voluntare. Acest consimțământ poate fi revocat în orice moment, cu efect ulterior printr-o notificare gratuită către **GYMBOLAND S.R.L.** Notificarea de revocare a consimțământului poate fi realizată spre exemplu prin e-mail către office@gymboland.ro sau la sediul social al societății. Vă rugăm să aveți în vedere faptul că revocarea consimțământului nu afectează legalitatea utilizării datelor înainte de retragerea consimțământului (notificarea nu are impact retroactiv). Dacă consimțământul nu este acordat sau a fost revocat, datele personale nu vor fi utilizate în scopurile de mai sus. În cazul în care aveți întrebări legate de această declarație de consimțământ sau de protecția datelor de către **GYMBOLAND S.R.L.** în general, vă rugăm să nu ezitați să ne contactați la adresa de e-mail: office@gymboland.ro

Puteți afla mai multe informații despre modalitatea în care **GYMBOLAND S.R.L.** procesează datele personale pe pagina noastră web: www.gymboland.ro precum și pe pagina facebook.com/gymboland.

Data completării:

Semnătură persoană vizată: _____

Anexa nr. 4

Informare privind utilizarea televiziunii video cu circuit închis (CCTV)

GYMBOLAND S.R.L. utilizează televiziune cu circuit închis (CCTV) în scopuri de siguranță. Păstrăm informațiile colectate de CCTV numai pentru o perioadă de timp care ne permite să ajutăm organele de reglementare și organele de aplicare a legii. Aceste informații sunt păstrate în medii sigure și accesul este rezervat numai personalului de securitate calificat.

În acest scop, realizăm monitorizarea video continuă a anumitor zone ale sediilor noastre, în special în incita locurilor de joacă pentru copii, precum și în jurul acestora (de exemplu, unele departamente de vânzări, parcare, depozite). Nu monitorizăm în locuri în care ar putea conduce la încălcarea confidențialității tale (de ex. toalete). De asemenea, nu folosim imaginea înregistrată în niciun alt scop și nu efectuăm analize suplimentare asupra acesteia. Accesul la înregistrări se acordă numai pentru un grup restrâns de angajați de încredere și nu sunt partajate cu nimeni, cu excepția autorităților competente, ca probe în scopul procedurilor judiciare. Am limitat timpul de stocare al înregistrărilor la 48 (patruzeci și opt) de ore și după această perioadă, acestea sunt suprascrise automat, fără posibilitatea de a fi reproduse.

GYMBOLAND
prin reprezentant legal

Anexa nr. 5

Act adițional privind activitățile de prelucrare a datelor cu caracter personal ale operatorului

ACT ADITIONAL

cu privire la Activitatile de Prelucrare a Datelor cu Caracter Personal ale

[denumirea Clientului]

Prezentul Act Aditional cu privire la activitatile de prelucrare a datelor cu caracter personal, denumit in continuare **"Act Aditional",** este incheiat la data de [ ], de catre si intre si face parte integranta din Contractul nr. [ ] din data de [ ]:

GYMBOLAND S.R.L., cu sediul social în București, Bd. Iuliu Manciu, nr. 7, sector 6, corp A, etajul 4, camera B30, număr de ordine în Registrul Comerțului: J40/8102/09.05.2008 atribuit pe data de 09.05.2008, identificator unic la nivel european (EUID): ROONRC.J40/8102/2008, cod unic de înregistrare: 23848390, denumita in continuare "**Operator"** sau "**Beneficiar"**

si

---- S.R.L., persoana juridica romana avand sediul in [ ], inregistrata la Registrul Comertului cu nr. [ ], avand cod fiscal [ ], reprezentata prin [ ], in calitate de [ ], denumita in continuare "**Imputernicit"** sau **"Furnizor",**

denumite in mod individual "**Partea**" sau in mod colectiv "**Partile**".

1. **Preambul**

1.1. Operatorul si Imputernicitul au incheiat un contract/contracte ("Contractul") pentru livrarea si/sau prestarea anumitor produse/servicii denumite in continuare "Serviciile", astfel cum sunt mentionate in Anexa nr. 1 la prezentul Acord de Prelucrare.

1.2. Prezentul Act Aditional, inclusiv anexele la acesta, constituie parte integranta din Contractul mentionat la clauza 1.1 de mai sus si inlocuieste si prevaleaza asupra oricaror alte prevederi sau clauze contractuale existente in Contract sau agreate de Parti, referitoare la prelucrarea Datelor Personale, incheiate inaintea datei Actului Aditonal.

1.3. Operatorul acorda o mare importanta protectiei Datelor Personale si s-a angajat sa protejeze toate datele personale ale angajatilor, furnizorilor, tertilor s.a.m.d. pe care le prelucreaza si, prin urmare, a implementat politici si proceduri menite sa asigure un nivel de protectie ridicat al acestora.

1.4. Prin urmare, Operatorul se asteapta de la toti furnizorii sai, de la angajatii, agentii, subcontractorii si colaboratorii acestora, sa adere la aceleasi standarde de protectie a Datelor Personale, pe de o parte, iar Imputernicitul declara ca accepta in mod expres prezentul Act Aditional, obligandu-se sa indeplineasca intocmai cerintele Operatorului cu privire la prelucrarea Datelor Personale ale sale, astfel cum este stabilit in prezentul Act Aditional, in cazul in care Imputernicitul colecteaza, utilizeaza, foloseste sau prelucreaza in orice maniera Date Personale ale Operatorului.

1.5. Prezentul Act Aditional priveste relatia contractuala dintre Operator si Imputernicit, astfel cum este aceasta reglementata prin Contract si urmare a careia Beneficiarul are calitatea de operator de date cu caracter personal pentru Datele Personale, astfel cum sunt definite in prezentul acord, avand controlul deplin asupra acestora, caz in care Furnizorul este imputernicit al Operatorului, in sensul art. 28 (1) din Regulamentul UE nr. 679/2016, Imputernicitul urmand a realiza prelucrarea in numele si pe baza instructiunilor Operatorului.

1.6. Fata de cele de mai sus, Operatorul a incheiat prezentul Act Aditional in baza garantiilor prezentate de catre Imputernicit, cu privire la punerea in aplicare si implementarea unor masuri tehnice si organizatorice adecvate, astfel incat operatiunile de prelucrare a Datelor Personale ale Beneficiarului, desfasurate de Imputernicit, sa indeplineasca in mod continuu cerintele Legislatiei Aplicabile si sa asigure protectia drepturilor Persoanelor Vizate.

1.7. Imputernicitul este de acord si garanteaza ca isi va indeplini obligatiile din Contract in conformitate cu cerintele Regulamentului si Legislatiei Aplicabile si ca va prelucra Datele Personale ale Operatorului in conformitate cu prezentul Act Aditional.

1.8. Prezentul Act Aditional intra in vigoare si este aplicabil incepand cu data semnarii acestuia de catre ambele Parti.

2. Definitii

2.1. "**Date Personale**" sau "**Datele Personale ale Operatorului**" inseamna orice date cu caracter personal, astfel cum sunt acestea definite in Regulament, furnizate de Operator sau colectate sau prelucrate de catre Imputernicit in numele Operatorului, in legatura cu Serviciile furnizate catre Operator prin Contractul sau Contractele mentionate in Anexa nr. 1, si orice alte date cu caracter personal prelucrate sub instructiunile Operatorului, in scopul indeplinirii Contractului sau Contractelor mentionate in Anexa nr. 1.

2.2. "**Legislatie Aplicabila**" inseamna oricare si toate legile si prevederile, normele de aplicare si reglementarile aplicabile prelucrarii datelor cu caracter personal, protectiei si securitatii acestora, orice modificari ulterioare, actualizari ale acestora si alte asemenea.

2.3. "**Data Actului Aditional**" inseamna data la care a fost incheiat prezentul document, astfel cum acest lucru este inscris pe prima pagina a acestuia.

2.4. "**Regulament**" inseamna Regulamentul nr. 679 din 27 aprilie 2016 privind protectia persoanelor fizice in ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a

acestor date si de abrogare a Directivei 95/46/CE, emis de Parlamentul European si Consiliul Uniunii Europene, care intra in vigoare la data de 25 mai 2018.

2.5. Denumirile de "**Operator**", "**Imputernicit**" sau "**Persoana Imputernicita de Operator**", "**Autoritate de Supraveghere**", "**Tari Terte**", "**Prelucrare**", "**Persoana Vizata**" vor avea aceeasi semnificatie cu cea definita si aratata in Regulament.

2.6. "**Incident de Securitate**" inseamna incalcarea securitatii datelor cu caracter personal, astfel cum aceasta este definita in Regulament.

2.7. "**Afiliati**" sau "**Membru Afiliat**" inseamna orice entitate juridica care controleaza sau este controlata de, sau are controlul comun cu, una dintre Partile acestui Act Aditional.

2.8. "**Subcontractor**" inseamna in prezentul Act Aditional orice imputernicit recrutat de catre Furnizor si orice subcontractor al acestuia care, dupa ce a fost autorizat de Operator, este de acord sa primeasca de la Imputernicit sau de la un subcontractor al acestuia orice Date Personale, exclusiv in scopul operatiunilor de prelucrare, care sa fie efectuate in numele si in conformitate cu instructiunile Operatorului in termenii si conditiile prezentul Act Aditional si in baza unui acord de subcontractare incheiat in acest scop. Oricare entitate care este membra a grupului de firme din care face parte Imputernicitul si care poate deveni implicata in derularea Serviciilor si in prelucrarea sau accesul doar la Datele Personale va fi, de asemenea, considerata Subcontractor.

2.9. Partile convin ca orice alti termeni folositi in prezentul Act Aditional si care nu au fost definiti in mod specific in prezentul document sa fie interpretati in conformitate cu terminologia si semnificatiile acestora din Regulament.

3. Detalii referitoare la Activitatile de Prelucrare

3.1. Operatorul autorizeaza Imputernicitul, doar in scopul si pe durata Contractului, sa prelucreze Datele Personale necesare pentru prestarea Serviciilor catre Operator. Detaliile cu privire la activitatile de prelucrare incredintate Imputernicitului sunt specificate in Anexa nr. 2 la prezentul Act Aditional.

3.2. Operatorul este de acord ca Imputernicitul sa prelucreze date despre apartenenta religioasa a angajatilor sai, in scopul acordarii zilelor libere cu ocazia sarbatorilor religioase, date despre starea de sanatate pentru inregistrarea concediilor medicale si de crestere a copilului, date medicale legate de medicina muncii. starea de sanatate pentru inregistrarea concediilor medicale si de crestere a copilului, date medicale legate de medicina muncii. Imputernicitul va cere aprobarea explicita a Operatorului pentru prelucrarea oricaror alte Date Personale, in plus fata de cele enumerate mai sus, care dezvaluie rasa sau originea etnica, optiuni politice, religioase, filosofice, sau apartenente la sindicate, sau date genetice, biometrice pentru scopul identificarii in mod unic al unei persoane, date privind sanatatea sau date privind viata sexuala sau orientarea sexuala, oricare dintre acestea.

1. Restrictii privind Activitatile de Prelucrare

1.1. Imputernicitul va asigura indeplinirea obligatilor sale in conformitate cu Legislatia Aplicabila pe costul propriu si nu va intreprinde nicio actiune de natura sa cauzeze o incalcare de catre Operator a Legislatiei Aplicabile.

1.2. Datele Personale vor fi prelucrate in conformitate cu principiile legate de prelucrarea datelor cu caracter personal, astfel cum sunt acestea prevazute in Legislatia Aplicabila si in conformitate cu instructiunile scrise de Operator.

1.3. Imputernicitul este de acord si garanteaza ca Datele Personale ale Operatorului sunt prelucrate in concordanta cu prezentul Act Aditional si cu instructiunile scrise primite din cand in cand de la Operator si ca vor fi accesate, folosite sau, in sens larg, prelucrate de catre Imputernicit numai in scopul indeplinirii de catre acesta din urma a obligatiilor contractuale din Contract. Imputernicitul:

(i) nu va obtine nici un fel de drepturi asupra Datelor Personale ca urmare a furnizarii Serviciilor, si

(ii) nu va transfera sau divulga Datele Personale, in tot sau in parte, nici unei terte parti, cu exceptia cerintelor impuse de prevederi legale, si

(iii) nu va prelucra sau folosi Datele Personale pentru scopuri proprii sau in beneficiul propriu.

1.4. Astfel, Imputernicitul se obliga:

(i) sa nu foloseasca Datele Personale, in tot sau in parte, pentru folosul propriu sau in folosul unui tert pentru nici un scop oricare ar fi acesta, atat pe durata, cat si dupa incetarea Contractului si Actului Aditional;

(ii) sa nu faca copii ale documentelor si/sau sistemelor informatice continand Date Personale, cu exceptia situatiei cand acest lucru este necesar pentru a furniza Serviciile, si nici sa nu divulge informatii referitoare sau in legatura cu Datele Personale catre terte parti;

2. Evidenta Activitatilor de Prelucrare

2.1. Imputernicitul este de acord si garanteaza ca intocmeste si pastreaza o evidenta (registru) a activitatilor de prelucrare desfasurate in numele Operatorului, care va contine cel putin urmatoarele informatii:

(a) numele si datele de contact ale Operatorului in numele caruia actioneaza Imputernicitul, ale reprezentantilor acestuia si ale responsabilului cu protectia datelor;

(b) tipul de date personale, categoriile de Persoane Vizate și de activitati de prelucrare desfasurate in numele Operatorului;

(c) informatii referitoare la personalul Imputernicitului si al oricarui Subcontractor cu rol de persoana imputernicita sau oricarei terte parti (persoana fizica sau juridica) care are acces la sau prelucreaza Datele Personale; aceasta va permite Operatorului, daca va fi cazul, (i) sa monitorizeze si (ii) sa verifice identitatea persoanelor care vor fi avut acces la si care vor fi prelucrat Datele Personale si (iii) sa introduca masuri de securitate si control;

(d) daca va fi cazul, transferurile Datelor Personale in tot sau in parte catre o tara terta sau organizatie internationala, inclusiv cu identificarea acestora, si in conditiile Regulamentului

si a Legislatiei Aplicabile, toate acestea in orce situatie numai cu respectarea clauzei 11 de mai jos;

(e) o descriere generala a masurilor tehnice si organizatorice menite sa asigure securitatea Datelor Personale.

2.2. Evidenta (registrul) activitatilor de prelucrare mentionata la clauza 5.1. de mai sus va fi tinuta in scris pe suport de hartie sau format electronic. Imputernicitul va pune la dispozitia Operatorului evidenta mentionata, precum si descrierea tuturor masurilor tehnice si organizatorice luate pentru protectia Datelor Personale, in conformitate cu Legislatia Aplicabila si prezentul Act Aditional. De asemenea, Imputernicitul va pune la dispozitia Autoritatii de Supraveghere la cererea acesteia respectiva evidenta, avand obligatia de a transmite imediat catre Operator o notificare (in max. 24 de ore) cu privire la aceasta.

3. Securitatea si Confidentialitatea Datelor Personale

3.1. Imputernicitul este de acord si garanteaza ca implementeaza masurile de protectie de ordin fizic, logistic, tehnic si organizationale necesare sa asigure protectia Datelor Personale, adaptate la riscurile activitatilor de prelucrare desfasurate, inclusiv, dar fara a se limita la, acele masuri impotriva distrugerii accidentale sau nelegale, pierderii sau modificarii/alterarii sau accesului neautorizat al Datelor Personale de catre terti.

3.2. In scopul clauzei 6.1. de mai sus, Imputernicitul este de acord si garanteaza implementarea a cel putin urmatoarelor masuri si, de asemenea, garanteaza ca se va asigura ca angajatii sai vor adera si se vor conforma la acestea:

3.2.1. toate persoanele autorizate sa prelucreze Datele Personale ale Operatorului in cadrul Serviciilor sunt subiectul unor angajamente ferme de confidentialitate sau a unor obligatii statutare privind confidentialitatea;

3.2.2. toate persoanele implicate in prestarea Serviciilor sunt informate, instruite si organizate, astfel incat sa fie asigurate garantii suficiente pentru protectia confidentialitatii si securitatii Datelor Personale. Imputernicitul va actualiza in mod constant instruirea si comunicarile catre angajatii sai care efectueaza activitati de prelucrare a Datelor Personale, in ceea ce priveste cerintele protectiei Datelor Personale si Legislatia Aplicabila.

3.2.3. luarea tuturor masurilor care sa previna orice folosire neadecvata sau frauduloasa a Datelor Personale, a documentelor sau informatiilor prelucrate, inclusiv, fara a se limita la:

(i) managementul accesului si autorizarii accesului, jurnalul de evenimente (event logging), securitatea stocarii Datelor Personale si a transmiterii (exchange) acestora,

(ii) pseudonimizarea sau criptarea Datelor Personale, a arhivelor si a copiilor de rezerva a datelor (data backup),

(iii) capacitatea de a asigura confidentialitatea, integritatea, disponibilitatea si rezistenta continue ale sistemelor si serviciilor de prelucrare a Datelor Personale ale Operatorului si a locatiilor in care sunt prelucrate aceste date,

(iv) capacitatea de a restabili disponibilitatea si accesul la Datele Personale ale Operatorului in timp util, in cazul in care are loc un incident de natura fizica sau tehnica, si efectuarea periodica si securizarea copiilor de rezerva (backups) a tuturor Datelor Personale ale Operatorului pe care Imputernicitul le are in posesie sau control,

(v) implementarea unui proces pentru testarea, evaluarea si auditarea periodice ale eficacitatii masurilor tehnice si organizatorice pentru a garanta securitatea prelucrarii Datelor Personale ale Operatorului;

(vi) orice alte masuri impuse de Legislatia Aplicabila.

3.3. Imputernicitul se obliga sa ia toate masurile necesare pentru a preintampina sau a face fata unui Incident de Securitate cu privire la Datele Personale ale Operatorului.

3.3.1. In cazul in care s-a produs un Incident de Securitate in legatura cu Datele Personale sau daca Imputernicitul are motive sa considere ca un astfel de incident s-a produs, Imputernicitul va notifica in mod prompt Operatorul intr-un termen de maxim 48 de ore de la momentul cand a luat la cunostinta despre aceasta.

3.3.2. Notificarea mentionata la clauza 6.3.1. de mai sus va fi transmisa cel putin pe e-mail la adresa ……. [adresa comunicata de client], avand subiectul: [numele Imputernicitului/ Incident de Securitate]. Este permisa notificarea telefonica in situatii urgente la numarul de telefon: ……, dar aceasta se considera neefectuata, daca nu este urmata in decursul termenului de 48 de ore de notificarea scrisa pe e-mail in conformitate cu prezenta clauza.

3.3.3. Notificarea mentionata la clauza 6.3.1. de mai sus va cuprinde cel putin urmatoarele informatii:

(i) o descriere a naturii Incidentului de Securitate si, pe cat posibil, a impactului acestuia asupora Datelor Personale, incluzand, de asemenea, sistemele afectate (daca sunt ale sau in legatura cu Operatorul), categoriile si numarul aproximativ al Persoanelor Vizate in cauza, precum si categoriile si numarul aproximativ al inregistrarilor de Date Personale in cauza;

(ii) numele si datele de contact ale responsabilului cu protectia datelor din partea Imputernicitului sau alt punct de contact pentru Imputernicit de unde se pot obtine mai multe informatii in acest sens;

(iii) o descriere a riscului astfel ivit si a posibilelor consecinte ale Incidentului de Securitate;

(iv) o descriere a masurilor luate sau propuse spre a fi luate de catre Imputernicit pentru a remedia problema Incidentului de Securitate, inclusiv, daca este potrivit, masurile pentru atenuarea efectelor sale negative.

3.3.4. Atunci cand situatia o impune sau nu este posibil, informatiile mentionate la clauza 6.3.3. de mai sus pot fi transmise de catre Imputernicit in mai multe etape, fara intarzieri nejustificate, dar intr-un interval maxim de 48 de ore de la momentul cand Imputernicitul a luat la cunostinta despre Incidentul de Securitate.

3.3.5. Imputernicitul este de acord si garanteaza ca va colabora cu Operatorul, astfel incat acesta din urma sa isi indeplineasca obligatiile sale de notificare a Autoritatii de Supraveghere cu privire la Incidentul de Securitate, in conformitate cu Regulamentul si Legislatia Aplicabila.

3.3.6. Imputernicitul nu va emite nici un fel de comunicat de presa sau orice astfel de comunicare publica in legatura cu un Incident de Securitate presupus sau care a avut efectiv loc si care implica Datele Personale ale Operatorului, fara acordul prealabil scris al Operatorului, cu exceptia situatiilor impuse de lege.

3.3.7. Imputernicitul va mentine inregistrari ale oricaror Incidente de Securitate cunoscute si care sunt in legatura cu Datele Personale ale Operatorului. Imputernicitul va pune la dispozitia Operatorului aceste inregistrari.

4. Subcontractori

4.1. Imputernicitul este de acord si garanteaza ca nu va implica nici un Subcontractor, furnizor sau orice membru afiliat grupului de companii din care face parte, in oricare dintre activitatile de prelucrare a Datelor Personale ale Operatorului, fara autorizarea prealabila specifica, generala, scrisa din partea Operatorului, cu respectarea obligatiilor de informare de la art. 28 alin. (2) din Regulament.

4.2. In cazul in care autorizarea mentionata la clauza 7.1. de mai sus este data de Operator, Imputernicitul este de acord si garanteaza ca acel contract sau act juridic pe care Imputernicitul il incheie cu Subcontractorul autorizat de Operator va contine cel putin acele obligatii ale Imputernicitului in legatura cu protectia datelor asumate prin prezentul Act Aditonal, astfel incat sa se asigure indeplinirea obligatiilor asumate de catre Imputernicit prin prezentul acord, in mod specific a obligatiilor a de a furniza garantii suficiente pentru implementarea masurilor tehnice si organizatorice adecvate. De asemenea, Imputernicitul se va asigura ca un astfel de contract sau act juridic incheiat cu un Subcontractor va inceta in mod automat la expirarea sau incetarea Contractului de Servicii dintre Operator si Imputernicit.

4.3. Imputernicitul este si va ramane raspunzator fata de Operator pentru conduita Subcontractorilor Imputernicitului in legatura cu Serviciile furnizate catre Operator si pentru orice consecinte materiale sau morale care deriva din aceasta conduita si, in general, pentru neindeplinirea sau indeplinirea defectuoasa de catre Subcontractor a obligatiilor subcontractate de protectie a Datelor Personale.

4.4. Imputernicitul se obliga sa transmita imediat catre Operator, la cerere acestuia din urma, o copie a contractului incheiat intre Imputernicit si Subcontractor, precum si o descriere a masurilor de securitate implementate de Subcontractor. Imputernicitul poate sa elimine din continutul contractului transmis orice fel de informatii comerciale referitoare la relatia dintre Imputernicit si Subcontractor, iar Operatorul isi asuma obligatia de a trata astfel de contracte cu maxima confidentialitate, cu exceptia situatiilor in care Operatorul este obligat sa divulge astfel de informatii sau documente catre o Autoritate de Supraveghere sau alta autoritate publica sau unei Persoane Vizate care solicita si este indreptatita la acest lucru.

4.5. In cazul in care Operatorul dispune de motive care determina ca acesta sa se opuna unui Subcontractor, pe motivul nerespectarii de catre acest Subcontractor a prezentului Act Aditional, Operatorul va notifica in scris Imputernicitul, iar Imputernicitul va depune eforturi rezonabile pentru a pune la dispozitia Operatorului o modificare cu privire la Subcontractor sau va recomanda o modificare rezonabila din punct de vedere comercial a activitatilor de prelucrare intr-o perioada de maxim 60 de zile de la data la care Operatorul si-a exprimat opozitia sau dezacordul. In cazul in care, in termenul dat, situatia nu este remediata de catre Imputernicit si/sau subcontractorul respectiv, Operatorul poate notifica Imputernicitul in scris cu privire la infirmarea autorizatiei acordate Subcontractorului cu efect imediat.

5. Persoanele Vizate. Solicitari si Asistenta.

5.1. Imputernicitul va indeplini in mod prompt orice instructiune a Operatorului referitoare la accesul, modificarea, transferul sau stergerea Datelor Personale ale Operatorului.

5.2. Imputernicitul se obliga sa informeze in scris Operatorul in maximum 3 (trei) zile lucratoare de la data primirii,

(i) cu privire la orice solicitare, cerere, plangere primita de Imputernicit de la o Persoana Vizata in legatura cu Datele Personale ale Operatorului prelucrate de Imputernicit, inclusiv, dar fara a se limita la: cereri de acces, de rectificare, stergere, opozitie, portabilitate, obiect sau nu al procesului decizional individual automatizat sau orice alte asemenea cereri, iar Imputernicitul se obliga sa nu raspunda la astfel de cereri sau solicitari, decat cu autorizarea expresa a Operatorului in acest sens;

(ii) in masura in care este permis de lege, cu privire la orice ordin administrativ sau judecatoresc, cerere, mandat, citatie sau orice alt document emis de o autoritate publica, prin care se solicita accesul sau divulgarea Datelor Personale ale Operatorului sau orice fel de detalii in legatura cu orice aspecte legate de acestea.

5.3. Imputernicitul va asista Operatorul si va colabora cu acesta in vederea indeplinirii cerintelor legale legate de protectia Datelor Personale in legatura cu cererile mentionate la clauza 8.2. de mai sus si Imputernicitul va asista Operatorul, prin masuri tehnice si organizatorice adecvate, in vederea indeplinirii obligatiei de a raspunde unor cereri de tipul celor mentionate la clauza 8.2. mai sus din partea Persoanelor Vizate sau autoritatilor publice.

5.4. Fata de cele mentionate la clauza 8.2., Imputernicitul va colabora pe deplin cu Operatorul, in masura permisa de lege, daca Operator doreste sa limiteze, conteste sau sa protejeze Datele Personale ale Operatorului impotriva unui astfel de acces sau divulgare.

6. Colaborare in vederea Conformarii

6.1. Imputernicitul declara ca este de acord si garanteaza ca va lua orice masuri cerute in mod rezonabil de Operator si va asista Operatorul in vederea asigurarii conformarii acestuia cu obligatiile referitoare la protectia Datelor Personale, in raport de Regulament si Legislatia Aplicabila si de politicile privind prelucrarea datelor personale definite de Operator.

6.2. Astfel, Imputernicitul il va asista pe Operator, la cererea acesteia din urma, cu privire la:

(i) securitate si notificarea Incidentelor de Securitate,

(ii) evaluarea riscurilor inerente activitatilor de prelucrare a Datelor Personale si implementarea masurilor de atenuare a acestora si asigurarea unui nivel adecvat de securitate a Datelor Personale, luandu-se in considerare stadiul tehnicii ("state of the art") si nivelul costurilor de implementare raportat la riscurile si categoriile de Date Personale care trebuie protejate,

(iii) efectuarea evaluarii impactului asupra protectiei datelor, inclusiv evaluarea riscurilor, si definirea masurilor de securitate si a mecanismelor de prevenire a acestor riscuri.

6.3. Imputernicitul este de acord si se obliga sa colaboreze cu Autoritatea de Supraveghere si Operator, in cazul in care cea din urma face obiectul unei investigatii, control sau alte asemenea proceduri din partea Autoritatii de Supraveghere.

7. Audit

7.1. Imputernicitul este de acord si garanteaza ca va pune la dispozitia Operatorului toate informatiile necesare in vederea demonstrarii conformitatii Imputernicitului cu obligatiile din prezentul Act Aditional si din Legislatia Aplicabila.

7.2. Astfel, Operatorul isi rezerva dreptul sa desfasoare orice verificare sau audit pe care il considera necesar in vederea verificarii conformarii Imputernicitului si a oricaror Subcontractori ai acestuia cu obligatiile prevazute in prezentul acord de Prelucrare, pe baza unei notificari scrise transmise Imputernicitului cu 20 zile inainte de efectuare. Operatorul va desfasura un astfel de audit sau verificare la o data agreata cu Imputernicitul, fara a afecta in mod semnificativ sau pe termen lung activitatea curenta a Imputernicitului.

7.3. Imputernicitul garanteaza ca va permite efectuarea de audituri (inclusiv inspectii) de catre Operator sau auditorii mandatati ai acestuia, in conditiile clauzei 10.2. si ca va participa la aceste audituri. In acest scop Imputernicitul:

(i) va permite accesul in locatiile (sediu, puncte de lucru etc.) Imputernicitului si va determina acelasi lucru in cazul Subcontractorilor sai; si

(ii) va furniza toate informatiile relevante si va permite accesul la toate echipamentele, software-urile, date, dosare, fisiere, sisteme informatice si la orice alte resurse de informatii folosite in legatura cu activitatile de prelucrare a Datelor Personale.

7.4. In cazul in care, in urma unei verificari sau audit, se constata ca Imputernicitul sau oricare dintre Subcontractorii acestuia nu a respectat oricare dintre garantiile sau obligatiile sale, Operatorul va solicita Imputernicitului sa ia masuri pentru remedierea respectivei incalcari, acordandu-i acestuia un termen de remediere.

7.5. Partile sunt de acord ca aceste operatiuni de verificare si auditare sau constatarile rezultate in urma acestora nu scutesc in nici un fel Imputernicitul de obligatiile sale contractuale in baza prezentului Act Aditional.

7.6. Imputernicitul declara ca este de acord si garanteaza ca va permite Operatorului sau va determina Subcontractorul sa permita Operatorului sau oricarui imputernicit al acestuia efectuarea unei

investigatii, verificari, audit sau inspectii in vederea certificarii indeplinirii obligatiilor de catre Imputernicit sau Subcontractor mentionate la clauza 12.3. de mai jos, in aceleasi conditii permise si garantate in prezenta clauza 10 din Actul Aditional.

8. Transferul International al Datelor Personale

8.1. Imputernicitul este de acord si garanteaza ca va efectua toate activitatile de prelucrare a Datelor Personale ale Operatorului exclusiv pe teritoriul U.E. si ca nu va transfera si nici nu va permite accesul la Datele Personale nici unei persoane fizice sau juridice localizate in tari terte, in sensul Regulamentului.

8.2. Imputernicitul aduce la cunostinta Operatorului, in scris, in Anexa nr. 2 locatiile geografice unde Datele Personale ale Operatorului sunt prelucrate de catre Imputernicit si de catre Subcontractor(i).

8.3. Imputernicitul se obliga sa informeze Operatorul cu privire la schimbari ale locatiilor geografice unde Serviciile sunt prestate si/sau unde Datele Personale sunt prelucrate in orice maniera sau de unde Subcontractorii acceseaza sau unde acestia prelucreaza Datele Personale, in contextul in care aceste schimbari au loc in cadrul teritoriului UE.

8.4. In cazul unei tari terte, in sensul Regulamentului, Imputernicitul se obliga sa furnizeze insusi sau sa obtina furnizarea din partea Subcontractorului a unui angajament cu privire la garantiile adecvate care vor guverna un astfel de transfer a Datelor Personale, in sensul celor specificate la art. 46 din Regulament, inclusiv incheierea de catre Imputernicit si/sau Subcontractorul respectiv si Operator a unui set de clauze standard de protectie a datelor personale, adoptate de Autoritatea de Supraveghere sau Comisia Europeana, dupa caz, in functie de Legislatia Aplicabila la acel moment.

9. Durata si Incetarea Acordului de Prelucrare. Obligatii.

9.1. Prezentul Act Aditional intra in vigoare la data semnarii lui si ramane valabil pe toate durata Contractului privind Serviciile, incheiat intre Parti. Cu toate acestea, Acordul de Prelucrare poate inceta si prin acordul de vointa al Partilor exprimat in scris sau in cazul in care Partile incheie un alt acord de prelucrare care sa inlocuiasca prezentul act aditional.

9.2. In cazul in care Imputernicitul nu isi indeplineste obligatiile din prezentul acord, Operatorul este indreptatit sa rezilieze prezentul Act Aditional la discretia sa, cu efect imediat de la data primirii notificarii de reziliere.

9.3. In cazul incetarii acestui Acord de Prelucrare pentru oricare cauza sau motiv, Imputernicitul este de acord si garanteaza ca, la instructiunile Operatorului si in conformitate cu Legislatia Aplicabila,

(i) va preda si returna in maximum 15 zile catre Operator Datele Personale, intr-un format utilizat in mod curent si agreat cu Operatorul, fara ca Imputernicitul sau Subcontractorii sa retina vreo copie integrala sau partiala a acestora, sau

(ii) va sterge in mod definitiv sau distruge sau va determina Subcontractorii sa stearga definitiv sau sa distruga Datele Personale si documentele si informatiile, mediile de stocare continand Datele Personale, precum si orice fisiere manuale sau computerizate care stocheaza Datele Personale si va transmite Operatorului o confimare in acest sens in termen de maxim [15 zile].

Clauza 10.6 de mai sus este aplicabila in acest caz.

10. Despagubiri si Raspundere

10.1. Imputernicitul va despagubi Operatorul pentru orice amenzi administrative impuse catre Operator de catre o autoritate de supraveghere, in sensul Regulamentului, pentru o presupusa incalcare a Legislatiei Aplicabile privind protectia Datelor Personale cauzate direct de nerespectarea de catre Imputernicit sau de catre oricare Subcontractor pe care Imputernicitul l-a angajat, a obligatiilor de prelucrare a Datelor Personale conform cu prezentul Acord de Prelucrare si Legislatia Aplicabila, in conditiile in care si numai dupa ce:

(i) o astfel de amenda este mentinuta de instantele competente in urma contestarii de catre Operator, si

(ii) Operatorul a informat in scris Imputernicitul despre actiunile autoritatii de supraveghere care au condus la sanctionarea Operatorului sau a informat in scris Imputernicitul imediat despre sanctiunile aplicate de autoritatea de supraveghere Operatorului si

(iii) o astfel de cauzalitate este stabilita de catre o instanta judecatoreasca in mod definitiv si irevocabil.

10.2. Daca Operatorul este tras la raspundere fata de o Persoana Vizata pentru incalcarea obligatiilor care îi revin în temeiul Legislatiei Aplicabile, in cazul in care o astfel de încalcare este imputabila direct indeplinirii necorespunzatoare sau neindeplinirii obligatiilor Imputernicitului sau a Subcontractorilor, Imputernicitul va plati Operatorului despagubiri pentru costurile si pierderile sale proportionale cu culpa sa. Imputernicitul va plati Operatorului costurile proportionale suportate de acesta din urma in legatura cu apararea sa, inclusiv, dar fara a se limita la taxe legale, onorariile, si orice daune, penalitati sau despagubiri, compensatii sau alte sume acordate de o instanta impotriva Operatorului, in conditiile in care si numai dupa ce

(i) o astfel de despagubire este acordata si mentinuta de instantele competente in mod definitiv si irevocabil, si

(ii) Operatorul a informat in scris Imputernicitul imediat ce a luat la cunostinta despre pretentiile si/sau actiunile intreprinse de Persoana Vizata in dovedirea unui posibil prejudiciu, permitand astfel Imputernicitului interventia in cauza respectiva in vederea apararii sale si

(iii) instanta judecatoreasca stabileste in mod definitiv si irevocabil indeplinirea necorespunzatoare sau neindeplinirea obligatiilor Imputernicitului ca fapt cauzator direct pentru tragerea la raspundere a Operatorului in acest fel.

11. Clauze Finale

11.1. **Punct de contact.** Imputernicitul se obliga si garanteaza ca desemneaza un singur punct de contact adecvat si specializat responsabil in vederea oferirii de raspunsuri la intrebarile, cererile si solicitarile Operatorului in legatura cu prelucrarea si protectia Datelor Personale. Acest punct de contact poate fi responsabilul cu protectia datelor din partea Imputernicitului, daca acesta a fost numit. Persoana indicata astfel va fi punctul principal de contact pentru responsabilul cu protectia datelor din partea Operatorului.

11.2. **Imbunatatirea continua a conditiilor de prelucrare si implicit a protectiei Datelor Personale.**

11.2.1. Partile sunt de acord ca pe intreaga durata a derularii Actului Aditional sa monitorizeze periodic stadiul si nivelul de protectie a Datelor Personale si cele mai bune practici relevante pentru imbunatatirea masurilor tehnice si organizatorice instituite in vederea asigurarii unui nivel de protectie corespunzator riscurilor asociate, si sa faca recomandari reciproce pentru imbunatatirea masurilor tehnice si organizatorice existente

11.2.2. In scopul prezentei clauze Partile convin sa aiba intalniri la cerere in vederea asigurarii schimbului de informatii si monitorizarii schimbarilor Legislatiei Aplicabile si practicii in materie sau aparitiei de noi reglementari in legatura cu acestea. In mod special, acestea pot viza: (i) introducerea unui Cod de Conduita aplicabil Imputernicitului, (ii) stabilirea unui mecanism de certificare care sa fie pus in practica de Imputernicit, (iii) stabilirea unui set de clauze standard care sa guverneze relatia dintre operatori si imputerniciti si (iv) stabilirea unor ghiduri si recomandari de catre Autoritatea de Supraveghere sau alte entitati cu putere in acest sens.

11.3. **Modificarea Actului Aditional.** Partile sunt de acord ca prezentul Act Aditional va putea fi modificat, suplimentat sau alte asemenea din cand in cand in functie de noile reglementari aparute in materia protectiei datelor personale sau in functie de cele mai bune practici in materie.

11.4. **Anexe.** Anexa nr. 1 sunt atasate la prezentul Act Aditional si fac parte integranta din acesta.

Prezentul Act Aditional a fost semnat de catre Parti , astazi [ ], in doua exemplare originale, cate unul pentru fiecare parte.

Semnaturi,

_____ _____

ANEXA NR. 1

la Actul Aditional cu privire la Activitatile de Prelucrare a Datelor cu Caracter Personal ale [denumirea clientului] din data de [ ]

In legatura cu art 1.1. din Actul Aditional, Partile declara ca intre ele au fost incheiate urmatoarele:

Contractul/ Contractele privind [ ] nr. [ ] din data de [ ], avand urmatoarele acte aditionale incheiate:

[*a se lista actele aditionale incheiate, daca este cazul*]

Semnaturi,

_____ _____

Anexa nr. 6

Notificare de încălcare a securității datelor cu caracter personal

I. Identificarea operatorului

1. Denumirea operatorului: GYMBOLAND S.R.L., cu sediul social în București, Bd. Iuliu Manciu, nr. 7, sector 6, corp A, etajul 4, camera B30, sectorul 6, număr de ordine în Registrul Comerțului: J40/8102/09.05.2008 atribuit pe data de 09.05.2008, identificator unic la nivel european (EUID): ROONRC.J40/8102/2008, cod unic de înregistrare: 23848390.
2. Punctul de contact de unde se pot obține informații:
   Nume și prenume:
   E-mail:
   Număr de telefon:
   Adresa de corespondență: București, Bd. Iuliu Manciu, nr. 7, sector 6, corp A, etajul 4, camera B30, sectorul 6.
3. Este o notificare nouă sau o completare a notificării inițiale?
   Notificare nouă:
   Completare notificării nr. _____ (*se va trece numărul de înregistrare al notificării din registrul general al Autorității de Supraveghere a Datelor cu Caracter personal*)

II. Informații privind încălcarea securității datelor cu caracter personal

4. Data și ora incidentului (dacă este necesar; dacă este necesar, se poate face o estimare) și ale depistării incidentului

4.1.Data și ora incidentului:
4.2. Data și ora depistării incidentului:

5. Caracterul încălcării securității datelor cu caracter personal (de exemplu: confidențialitate/integritate/disponibilitate)

6. Natura și conținutul datelor cu caracter personal în cauză

7. Măsuri tehnice și organizatorice aplicate sau care urmează a fi aplicate

8. Utilizarea relevantă a altor operatori (dacă este cazul)

9. Rezumatul incidentului care a generat încălcarea securității datelor cu caracter personal (inclusiv localizarea fizică a încălcării și suporturile de stocare implicate)

10. Numărul persoanelor fizice vizate (estimare, după caz)

11. Eventualele consecințe și efecte adverse (riscuri) pentru persoanele fizice vizate

12. Măsurile tehnice și organizatorice luate de operator în scopul atenuării eventualelor efecte negative

13. Conținutul informării sau motivele pentru care nu s-a făcut informare persoanelor fizice vizate

14. Mijloacele de comunicare utilizate pentru transmiterea informărilor

15. Numărul persoanelor fizice vizate

16. Încălcare a securității datelor cu caracter personal care implică persoane fizice vizate din alte state membre

Da:
Nu:

17. Notificarea altor autorități naționale competente
Da:
Nu:
Dacă da, menționați autoritățile competente

Data:
Semnătura reprezentantului operatorului: