POLITICA DE SECURITATE
a prelucrărilor de date cu caracter personal

1. SCOP

1.1. TRAVELIO GROUP ROMANIA S.R.L. va fi denumită în continuare "TGR" sau "Operatorul".

1.2. Scopul prezentei politici este de a stabili măsurile necesare şi responsabilităţile angajaţilor TGR şi/sau persoanelor împuternicite de către TGR pentru îndeplinirea obligaţiilor referitoare la garantarea şi protejarea drepturilor şi libertăţilor fundamentale ale persoanelor fizice, în special a dreptului la viaţa intimă, familială şi privată, cu privire la prelucrarea datelor cu caracter personal.

1.3. Prezentul document completează şi precizează obligaţiile privind protecţia datelor cu caracter personal şi se aplică tuturor activităţilor legate de relaţiile contractuale stabilite cu terţe părţi, în cadrul cărora angajaţii TGR şi/sau persoanele împuternicite de către TGR prelucrează date cu caracter personal.

2. DOMENIUL DE APLICARE

Prezenta politică se aplică tuturor angajaţilor TGR cu atribuţii de prelucrare a datelor cu caracter personal şi/sau, după caz, persoanelor împuternicite.

3. TERMENI ŞI DEFINIŢII

În sensul prezentei politici, termenii de mai jos au următoarea semnificaţie:

a) "ANSPDCP" = Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal;

b) "Codul numeric personal" (CNP) = un număr semnificativ care individualizează în mod unic o persoană fizică, constituind un instrument de verificare a stării civile a acesteia şi de identificare în anumite sisteme informatice de către persoanele autorizate;

c) "Date cu caracter personal" = informaţii 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 identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

d) "Date cu caracter personal cu funcţie de identificare de aplicabilitate generală" (date cu caracter special) = numere prin care se identifică o persoană fizică în anumite sisteme de evidenţă şi care au aplicabilitate generală, cum ar fi: codul numeric personal, seria şi numărul actului de identitate, numărul paşaportului, al permisului de conducere, numărul de asigurare socială sau de sănătate;

e) "Date anonime" = date care, datorită originii sau modalităţii specifice de prelucrare, nu pot fi asociate cu o persoană identificată sau identificabilă;

f) "Persoana vizată" = persoana fizică la care se referă datele cu caracter personal prelucrate;

g) "Operator" = orice persoană fizică/juridică, de drept privat ori de drept public, inclusiv autorităţile publice, instituţiile şi structurile teritoriale ale acestora, care stabileşte scopul şi mijloacele de prelucrare a datelor cu caracter personal; dacă scopul şi mijloacele de prelucrare a datelor cu caracter personal sunt determinate printr-un act normativ sau în baza unui act normativ, operator este persoana fizică sau juridică, de drept public ori de drept privat, care este desemnată ca operator prin acel act normativ sau în baza acelui act normative;

h) "Persoană împuternicită de operator" = o persoană fizică sau juridică, de drept privat ori de drept public, inclusiv autorităţile publice, instituţiile şi structurile teritoriale ale acestora, care prelucrează date cu caracter personal pe seama operatorului;

i) "Persoana responsabilă de politica de securitate a datelor cu caracter personal" = persoana responsabilă de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei care conţine date cu caracter personal, precum şi de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a deţinătorului de date cu caracter personal;

j) "Prelucrarea datelor cu caracter personal" sau "Prelucrarea datelor" = orice operaţiune sau set de operaţiuni 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 dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;

k) "Stocarea" = păstrarea pe orice fel de suport a datelor cu caracter personal colectate;

l) "Utilizator" = orice persoană care acţionează sub autoritatea operatorului, a persoanei împuternicite sau a reprezentantului, cu drept recunoscut de acces la bazele de date cu caracter personal;

m) "Parte terţă" = o persoană fizică sau juridică, autoritate publică, agenţie sau organism, altul decât persoana vizată, operatorul, persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

n) "Încălcarea securităţii datelor cu caracter personal" = o încălcare a securităţii 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. Constatarea acestei stări de fapt, reprezintă în fapt constatarea unui "incident de securitate" sau "incidentul";
o) SEE" = Spaţiu Economic European;
p) "Ţară terţă" = orice ţară din afara UE/SEE, cu excepţia cazului în care respectiva ţară face obiectul unei decizii valabile de adecvare a Comisiei Europene privind protecţia Datelor cu caracter personal în ţări terţe.

4. DOCUMENTE DE REFERINŢĂ

a) Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare;
b) Ordinul Avocatului Poporului nr. 52 din 18/04/2002 privind aprobarea Cerinţelor minime de securitate a prelucrărilor de date cu caracter personal;
c) Decizia ANSPDCP nr. 52/2012 privind prelucrarea datelor cu caracter personal prin utilizarea mijloacelor de supraveghere video;
d) Decizia ANSPDCP nr. 90 din 18/07/2006 privind stabilirea cazurilor în care nu este necesară notificarea prelucrării unor date cu caracter personal;
e) Decizia ANSPDCP nr. 100 din 23/11/2007 privind stabilirea cazurilor în care nu este necesară notificarea prelucrării unor date cu caracter personal;
f) Decizia ANSPDCP nr. 132 din 20/12/2011 privind condiţiile prelucrării codului numeric personal şi a altor date cu caracter personal având o funcţie de identificare de aplicabilitate generală;
g) Regulamentul European 2016/679 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

5. PRECIZĂRI

5.1. Reguli generale

5.1.1. Prin cerinţe minime de securitate este avut în vedere un complex de măsuri tehnice, informatice, organizatorice, logistice, proceduri şi politici de securitate prin care să se asigure nivelul minim de securitate prevăzut în art. 20 din Legea nr. 677/2001, în conformitate cu cerinţele minime de securitate a prelucrărilor de date cu caracter personal, aprobate prin Ordinul 52 din 18 Aprilie 2002 ale Avocatului Poporului.

5.1.2. TGR s-a angajat să adoptate măsuri tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerilor accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat. În acest sens a fost desemnat, la nivelul TGR, persoană responsabilă cu respectarea dispoziţiilor Legii nr.677/2001, Administratorul societăţii, respectiv doamna David Adriana-Claudia, cu următoarele date de contact:

- Adresa de corespondenţă: Bld. Corvin nr. 5 bis, bl. 105, sc. A, ap. 3, parter, 331010, Hunedoara, jud. Hunedoara
- Telefon: 0721 321 002
- E-mail: gdpr@travelioromania.ro

5.1.3. TGR a luat şi va lua în permanenţă măsuri de stocare în siguranţă a informaţiilor privind date cu caracter personal, astfel încât să fie asigurat un nivel adecvat de protecţie şi securitate, în sensul Legii 677/2001.

5.1.4. Pentru îndeplinirea prevederilor legale aferente şi în vederea satisfacerii cerinţelor păstrării în siguranţă a datelor şi informaţiilor, societatea a elaborat şi implementat măsuri organizatorice şi tehnice orientate pe anumite direcţii de acţiune:

a) identificarea şi autentificarea utilizatorului;
b) tipul de access;
c) colectarea datelor;
d) execuţia copiilor de siguranţă;
e) computerele şi terminalele de access;
f) fişierele de access;
g) sistemele de telecomunicaţii;
h) instruirea personalului;
i) folosirea computerelor;
j) imprimarea datelor;
k) prelucrarea manuală a datelor cu caracter personal.

5.2. Proceduri specifice

5.2.1. **Identificarea şi autentificarea utilizatorului**

Pentru a primi acces la datele cu caracter personal, utilizatorii trebuie sa se autentifice în sistemele informatice ale TGR. Autentificarea în cadrul sistemelor informatice ale societăţii se face prin introducerea parolelor de autentificare, unice şi netransmisibile, pe bază de roluri. Fiecare utilizator va avea propriul său cod de identificare (nume de utilizator); niciodată nu va fi alocat acelaşi cod de identificare mai multor utilizatori şi acesta nu poate fi partajat către mai multe persoane. Codurile de identificare sau conturile de utilizator nefolosite o perioadă mai îndelungată sunt dezactivate şi distruse după un control prealabil. Perioada după care sunt dezactivate şi distruse acestea este stabilită prin politicile societăţii. Parolele sunt schimbate periodic, numai de către utilizatorii autorizaţi, conform politicii societăţii cu privire la administrarea şi gestionarea conturilor de utilizator.

5.2.2. **Tipul de acces**

Utilizatorii trebuie să acceseze numai datele cu caracter personal necesare pentru îndeplinirea atribuţiilor lor de serviciu. Pentru aceasta trebuie să fie stabilite tipurile de acces după funcţionalitate (administrare, introducere, prelucrare, salvare etc.) şi după acţiuni aplicate asupra datelor cu caracter personal (scriere, citire, ştergere), precum şi procedurile privind aceste tipuri de acces. Compartimentul care asigură suportul tehnic poate avea acces la datele cu caracter personal pentru

rezolvarea incidentelor şi a problemelor apărute în utilizarea sistemelor informatice. Alte măsuri specifice pentru controlul accesului sunt:

a) în spaţiile destinate desfăşurării activităţii firmei sunt instalate sisteme de alarmă antiefracţie;
b) monitorizarea şi intervenţia în caz de alarmă sunt asigurate de o societate de protecţie şi pază.

5.2.3. **Colectarea datelor**

TGR desemnează utilizatori autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal în sistemele informaţionale . Orice modificare a datelor cu caracter personal trebuie să se poate face numai de către utilizatori autorizaţi desemnaţi. TGR va lua măsuri pentru ca sistemele informaţionale să înregistreze cine a făcut modificarea datelor cu caracter personal, data şi ora modificării. Pentru o mai bună administrare, vor fi implementate măsuri pentru ca sistemele informaţionale să menţină datele şterse sau modificate.

5.2.4. **Execuţia copiilor de siguranţă**

TGR a stabilit intervalul de timp la care se vor executa copiile de siguranţă ale bazelor de date ce conţin date cu caracter personal. Utilizatorii care execută aceste proceduri sunt într-un număr restrâns sau este un singur utilizator, desemnat de către TGR prin politici proprii. Copiile de siguranţă se stochează pe un dispozitiv distinct faţă de cel pe care se află baza de date cu caracter personal. Sistemele/dispozitivele care gestionează datele cu caracter personal trebuie sa fie protejate prin sistemul de backup periodic împotriva pierderii sau distrugerii datelor sau a sistemului informatic.

5.2.5. **Computerele şi terminalele de acces**

Computerele şi alte terminale de acces la date cu caracter personal aflate în sediul TGR vor fi instalate în încăperi cu acces restricţionat şi/sau accesate numai pe bază de parola de conectare/acces în dispozitivul/computerul respectiv. Unde nu pot fi asigurate aceste condiţii, computerele/alte terminale vor fi instalate/depozitate în încăperi care se pot încuia. Dacă pe ecran apar date cu caracter personal asupra cărora nu se acţionează o perioadă dată, stabilită de către TGR, sesiunea de lucru se va închide automat. Mărimea acestei perioade se determină în funcţie de operaţiile care trebuie executate. Terminalele de acces folosite în relaţia cu publicul, pe care apar date cu caracter personal, vor fi poziţionate astfel încât să nu poată fi văzute de public şi după o perioadă scurtă, stabilită de TGR, în care nu se acţionează asupra lor, acestea vor fi ascunse sau sesiunea de lucru va fi închisă. Nu este permisă scoaterea din societate a mediilor de stocare mobile (CD/DVD, USB Stick, Portable HDD) care conţin date cu caracter personal, decât cu aprobare prealabilă din partea conducerii societăţii.

5.2.6. **Fişierele de acces**

TGR ia măsuri pentru ca orice accesare a bazei de date cu caracter personal să fie înregistrată. Pentru prelucrările automate, aceste informaţii sunt stocate într-un fişier de acces general sau în fişiere separate pentru fiecare utilizator. Orice încercare de acces neautorizat va fi, de asemenea, înregistrată. TGR păstreaza fişierele de acces cel puţin 2 ani, pentru a fi folosite ca probe în cazul unor investigaţii. Dacă investigaţiile se prelungesc, aceste fişiere se vor păstra atât timp cât se va considera necesar. Fişierele de acces fac posibilă identificarea de către TGR sau de către persoană împuternicită, a persoanelor care au accesat date cu caracter personal fără un motiv anume, în vederea aplicării unor sancţiuni sau a sesizării organelor competente.

5.2.7. **Sistemele de telecomunicaţii**

TGR face periodic revizuirea conturilor de utilizatori şi a privilegiilor acordate, pentru detectarea unor disfuncţionalităţi în ceea ce priveşte sistemele informaţionale. Sistemele informaţionale vor fi concepute astfel încât datele cu caracter personal să nu poată fi interceptate sau transmise de oriunde. Prin sistemele de telecomunicaţii, datele cu caracter personal vor fi transmise printr-un canal sigur. Datele cu caracter personal transferate în zonele de securitate externă sau nesigură vor fi criptate.

5.2.8. **Instruirea personalului**

Personalul TGR este informat cu privire la prevederile Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, la cerinţele minime de securitate a prelucrărilor de date cu caracter personal, precum şi cu privire la riscurile pe care le comportă prelucrarea datelor cu caracter personal. Utilizatorii care au acces la date cu caracter personal vor fi instruiţi asupra confidenţialităţii acestora. Utilizatorii sunt obligaţi să îşi închidă sesiunea de lucru atunci când părăsesc locul de muncă.

5.2.9. **Folosirea computerelor**

Pentru menţinerea securităţii prelucrării datelor cu caracter personal (în special împotriva viruşilor informatici) trebuie luate măsuri privind:

a) interzicerea folosirii de către utilizatori a programelor software care provin din surse neverificate;
b) informarea utilizatorilor în privinţa pericolului privind viruşii informatici;
c) implementarea unor sisteme automate de tip antivirus şi protecţie malware şi de securitate a sistemelor informatice;
d) dezactivarea posibilităţii de copiere sau imprimare a datelor cu caracter personal afişate pe ecran în afara fluxurilor normale de afaceri.

5.2.10. **Imprimarea datelor**

Imprimarea datelor cu caracter personal se va realiza doar de către utilizatorii autorizaţi de către TGR.

5.2.11. **Prelucrarea manuală a datelor cu caracter personal**

Documentele care conţin date cu caracter personal vor fi ţinute în fişete sau dulapuri închise cu cheie sau cu un alt mecanism de securizare. Documentele care conţin date cu caracter personal, folosite pentru realizarea anumitor operaţiuni se vor preda persoanelor abilitate sau se vor închide imediat după terminarea acestora.

5.3. Principiile care stau la baza prelucrarii datelor cu caracter personal

Prelucrarea datelor cu caracter personal se realizează cu respectarea cerințelor legale și în condiții care să asigure securitatea, confidențialitatea și respectarea drepturilor persoanelor vizate. Prelucrarea datelor cu caracter personal se face cu respectarea următoarelor principii:

a) legalitatea: prelucrarea datelor cu caracter personal se face în temeiul și în conformitate cu prevederile legale;

b) scopul bine determinat: orice prelucrare de date cu caracter personal se face în scopuri bine determinate, explicite și legitime, adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate și ulterior prelucrate;
c) confidențialitatea: persoanele care prelucrează, în numele TGR date cu caracter personal au prevăzut în fișa postului, anexa la contractul individual de munca, o clauză de confidențialitate;
d) consimţământul persoanei vizate: orice prelucrare de date cu caracter personal, cu excepția prelucrărilor care vizează date din categoriile strict menționate în Legea 677/2001, poate fi efectuată numai dacă persoana vizată și-a dat consimţământul în mod expres și neechivoc pentru acea prelucrare;
e) informarea: persoanele vizate iau cunostinţă despre faptul că li se vor prelucra date cu caracter personal;
f) protejarea persoanelor vizate: drepturile persoanei vizate sunt prevăzute la art. 5.6.
g) securitatea: măsurile de securitate a datelor cu caracter personal sunt stabilite astfel încât să asigure un nivel adecvat de securitate a datelor cu caracter personal procesate.

5.4. Prelucrarea datelor cu caracter personal având o funcţie de identificare de aplicabilitate generală, inclusiv dezvăluirea acestora către terţi, se face numai în urmatoarele condiţii:

a) persoana vizată și-a dat în mod expres consimţământul; sau
b) prelucrarea este prevăzută în mod expres de o dispoziţie legală; sau
c) în alte cazuri, cu avizul Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal şi numai cu condiţia instituirii unor garanţii adecvate pentru respectarea drepturilor persoanelor vizate.

5.4.1. TGR respectă principiul caracterului adecvat, pertinent şi neexcesiv, precum şi măsurile de confidenţialitate şi de securitate a prelucrărilor. În cazul prevazut la punctul c) de mai sus, se au în vedere urmatoarele aspecte:

a) scopul prelucrării să fie determinat, explicit şi legitim;
b) stabilirea şi aplicarea unor măsuri prin care să se asigure exercitarea drepturilor persoanelor vizate;
c) durata de stocare a datelor să fie pe perioada strict necesară îndeplinirii scopului, după care datele vor fi şterse sau distruse, după caz;
d) stabilirea modalităţilor de acces la sistemele de evidenţă în vederea colectării datelor, în funcţie de care se vor stabili şi respecta măsuri tehnice şi organizatorice adecvate pentru protejarea datelor;
e) utilizarea datelor numai în limitele scopului stabilit;
f) dezvăluirea către alţi destinatari este interzisă, cu excepţia situaţiei în care există consimţământul persoanei vizate sau o prevedere legală expresă;
g) desemnarea, în scris, a persoanei/persoanelor care va/vor prelucra datele şi care trebuie să îşi asume răspunderea păstrării confidenţialităţii acestora, lista conţinând evidenţa acestor persoane fiind actualizată ori de câte ori se impune;
h) numirea, în scris, a unei persoane specializate în securitatea informaţiei care să vegheze la prelucrarea datelor, inclusiv la buna funcţionare a sistemelor informatice utilizate în această activitate;
i) stabilirea unui plan de securitate a informaţiilor care să cuprindă, în principal, securitatea tehnică pe plan informatic şi securitatea spaţiilor în care se prelucrează datele, ţinând cont de cerinţele minime de securitate;
j) stabilirea, în scris, a drepturilor şi obligaţiilor operatorului care transmite datele şi ale operatorului care le primeşte.

5.4.2. Colectarea şi prelucrarea datelor cu caracter personal având o funcţie de identificare de aplicabilitate generală, inclusiv dezvăluirea acestora, prin efectuarea şi reţinerea de copii de pe cartea de identitate sau de pe documente care le conţin, sunt interzise, cu excepţia situaţiilor prevăzute la art. 5.4., alin. a), b) si c) de mai sus.

5.5. Prelucrarea datelor cu caracter personal prin utilizarea sistemelor de supraveghere video

5.5.1. Prelucrarea datelor cu caracter personal prin utilizarea sistemelor de supraveghere video se efectuează cu respectarea regulilor generale prevăzute de art. 4 din Legea nr. 677/2001, cu modificările şi completările ulterioare. Camerele de supraveghere video, dacă există, sunt montate în locuri vizibile. Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se va face pentru realizarea unor interese legitime, fără a se prejudicia drepturile şi libertăţile fundamentale sau interesul persoanelor vizate. Nu este permisă prelucrarea datelor cu caracter personal ale angajaţilor prin mijloace de supraveghere video în interiorul spaţiilor/birourilor unde aceştia îşi desfăşoară activitatea la locul de muncă, cu excepţia situaţiilor prevăzute expres de lege sau a avizului ANSPDCP. TGR, în calitate de operator care prelucrează date cu caracter personal prin mijloace de supraveghere video este obligat să furnizeze informaţiile prevăzute la art. 12 alin. (1) din Legea nr. 677/2001, cu modificările şi completările ulterioare, inclusiv cu privire la:

a) existenţa sistemului de supraveghere video şi scopul prelucrării datelor prin astfel de mijloace;
b) identitatea operatorului;
c) existenţa înregistrării imaginilor şi categoriile de destinatari ai acestora;
d) drepturile persoanelor vizate şi modul de exercitare a acestora.

5.5.2. Informaţiile mentionate mai sus trebuie aduse la cunoştinţa persoanelor vizate, în mod clar şi permanent. Existenţa sistemului de supraveghere video este semnalată prin intermediul unei pictograme care conţine o imagine reprezentativă cu vizibilitate suficientă şi poziţionată la o distanţă rezonabilă de locurile unde sunt amplasate echipamentele de supraveghere video. Prelucrarea datelor cu caracter personal prin mijloace de supraveghere video se poate realiza doar de către persoanele autorizate de către TGR (personal propriu sau persoane împuternicite de către operator), instruite cu privire la legislaţia referitoare la protecţia datelor cu caracter personal şi obligate să se supună acesteia. Durata de stocare a datelor obţinute prin intermediul sistemului de supraveghere video este proporţională cu scopul pentru care se prelucrează datele, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate. La expirarea termenului stabilit, înregistrările se distrug sau şterg, după caz, în funcţie de suportul pe care s-au stocat.

5.6. Drepturile persoanelor ale căror date personale sunt colectate şi/sau prelucrate

5.6.1. **Dreptul de a fi informat**

5.6.1.1. În cazul în care datele cu caracter personal sunt obţinute direct de la persoana vizată, TGR este obligată să furnizeze persoanei vizate cel puţin următoarele informaţii, cu excepţia cazului în care această persoană posedă deja informaţiile respective:

a) scopul în care se face prelucrarea datelor;
b) informaţii suplimentare, precum: destinatarii sau categoriile de destinatari ai datelor; dacă furnizarea tuturor datelor cerute este obligatorie şi consecinţele refuzului de a le furniza;
c) existenţa drepturilor prevăzute de lege pentru persoana vizată, în special a dreptului de acces, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile în care pot fi exercitate;
d) orice alte informaţii a căror furnizare este impusă prin dispoziţie a autorităţii de supraveghere, ţinând seama de specificul prelucrării.

5.6.1.2. Pe pagina de internet a TGR (www.travelioromania.ro) este postată "Politica de confidenţialitate".
5.6.1.3. Înainte de completarea datelor cu caracter personal se solicită consimţământul persoanelor vizate, pentru prelucrarea acestora.
5.6.1.5. Clădirile care sunt supravegheate video vor avea, la intrare, afişat în loc vizibil, informarea privind preluarea şi stocarea de imagini.
5.6.2. **Dreptul de acces la date**
Orice persoană vizată are dreptul de a obţine de la TGR (în calitate de operator), la cerere şi în mod gratuit pentru o solicitare pe an, confirmarea faptului că datele care o privesc sunt sau nu sunt prelucrate de acesta.
TGR este obligat, în situaţia în care prelucrează date cu caracter personal care privesc solicitantul, să comunice acestuia, împreună cu confirmarea, cel puţin următoarele:

a) informaţii referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;
b) comunicarea într-o formă inteligibilă a datelor care fac obiectul prelucrării, precum şi a oricărei informaţii disponibile cu privire la originea datelor;
c) informaţii asupra principiilor de funcţionare a mecanismului prin care se efectuează orice prelucrare automată a datelor care vizează persoana respectivă;
d) informaţii privind existenţa dreptului de intervenţie asupra datelor şi a dreptului de opoziţie, precum şi condiţiile în care pot fi exercitate;
e) informaţii asupra posibilităţii de a înainta plângere către autoritatea de supraveghere, precum şi de a se adresa instanţei pentru atacarea deciziilor operatorului, în conformitate cu dispoziţiile legii.

Notă:
(1) Persoana vizată poate solicita de la TGR informaţiile prevăzute de lege, printr-o cerere de exercitare întocmită în formă scrisă, semnată şi înregistrată la registratura societăţii. În cerere, solicitantul poate arăta dacă doreşte ca informaţiile să îi fie comunicate la o anumită adresă, care poate fi şi de poştă electronică, sau printr-un serviciu de corespondenţă care să asigure că predarea i se va face numai personal.
(2) TGR este obligată să comunice informaţiile solicitate, în termen de 30 de zile calendaristice de la data primirii cererii, cu respectarea eventualei opţiuni a solicitantului.
5.6.3. **Dreptul de intervenţie asupra datelor**
Orice persoană vizată are dreptul de a obţine de la operator, la cerere şi în mod gratuit:

a) după caz, rectificarea, actualizarea, blocarea sau ştergerea datelor a căror prelucrare nu este conformă legii, în special a datelor incomplete sau inexacte;
b) după caz, transformarea în date anonime a datelor a căror prelucrare nu este conformă legii.

5.6.4. **Dreptul de opoziţie**
Persoana vizată are dreptul de a se opune în orice moment, din motive întemeiate şi legitime legate de situaţia sa particulară, ca date care o vizează să facă obiectul unei prelucrări, cu excepţia cazurilor în care există dispoziţii legale contrare. În caz de opoziţie justificată prelucrarea nu mai poate viza datele în cauză.
5.6.5. **Dreptul de a nu fi supus unei decizii individuale**
5.6.5.1. Orice persoană are dreptul de a cere şi de a obţine retragerea/ anularea/ reevaluarea oricărei decizii care produce efecte juridice în privinţa sa, adoptată exclusiv pe baza unei prelucrări de date cu caracter personal, efectuată prin mijloace automate, destinată să evalueze unele aspecte ale personalităţii sale, precum competenţa profesională, credibilitatea, comportamentul său ori alte asemenea aspecte.
5.6.5.2. Respectându-se celelalte garanţii prevăzute de lege, o persoană poate fi supusă unei decizii de natura celei vizate la alin. 5.6.5.1, numai în următoarele situaţii:

a) decizia este luată în cadrul încheierii sau executării unui contract, cu condiţia ca cererea de încheiere sau de executare a contractului, introdusă de persoana vizată, să fi fost satisfăcută sau ca unele măsuri adecvate, precum posibilitatea de a-şi susţine punctul de vedere, să garanteze apărarea propriului interes legitim;
b) decizia este autorizată de o lege care precizează măsurile ce garantează apărarea interesului legitim al persoanei vizate.

5.6.6. **Dreptul de a se adresa justiţiei**
5.6.6.1. Fără a se aduce atingere posibilităţii de a se adresa cu plângere Autorităţii de Supraveghere, persoanele vizate au dreptul de a se adresa justiţiei pentru apărarea oricăror drepturi garantate de lege, care le-au fost încălcate.
5.6.6.2. Orice persoană care a suferit un prejudiciu în urma unei prelucrări de date cu caracter personal, efectuată ilegal, se poate adresa instanţei competente pentru repararea acestuia.
5.7. Comunicarea datelor cu caracter personal
5.7.1. Datele cu caracter personal se pot comunica între TGR şi împuterniciţii acestuia sau între TGR sau împuterniciţi ai acestuia şi alte instituţii ori organisme publice sau entităţi de drept public sau privat în una dintre următoarele situaţii:

a) dacă persoana vizată şi-a dat consimţământul expres şi neechivoc pentru comunicarea datelor sale;

b) fără consimţământul persoanei vizate în cazurile prevăzute de lege.

5.7.2. Comunicarea datelor cu caracter personal în situaţiile prevăzute la alin. 5.7.1. se poate face dacă este îndeplinită una dintre următoarele condiţii:

a) comunicarea se efectuează pe baza unui contract sau, după caz, a unui document de cooperare care trebuie să cuprindă cel puţin: numărul de înregistrare a notificării, temeiul legal al prelucrării şi scopul acesteia, termenul maxim de prelucrare, drepturile şi obligaţiile părţilor, modalităţile de asigurare a securităţii prelucrărilor şi de respectare a drepturilor persoanei vizate, precum şi menţiunea că datele pot fi utilizate doar de structura beneficiară şi numai în scopul pentru care au fost solicitate;
b) comunicarea se efectuează în baza unei solicitări scrise, care trebuie să cuprindă temeiul legal, scopul prelucrării şi datele solicitate, precum şi, dacă este cazul, numărul atribuit beneficiarului de Autoritatea Naţională de Supraveghere.

5.7.3. Comunicarea datelor cu caracter personal se poate face şi on-line, cu respectarea dispoziţiilor alin. 5.7.1. şi 5.7.2. şi asigurarea securităţii sistemelor de comunicaţii a datelor cu caracter personal.

5.7.4. Datele cu caracter personal asupra cărora persoanele vizate au exercitat şi li s-a recunoscut dreptul de opoziţie nu pot face obiectul prelucrării.

5.7.5. Cererile pentru comunicarea datelor cu caracter personal TGR trebuie să conţină datele de identificare a solicitantului, precum şi motivarea şi scopul cererii, conform prevederilor legale.

5.7.6. Cererile care nu conţin aceste elementele se restituie pentru completare, iar cele care nu se încadrează în condiţiile prevăzute de lege se resping, menţionându-se motivele pentru care comunicarea datelor cu caracter personal nu este posibilă.

5.7.7. Înainte de comunicarea datelor cu caracter personal, TGR verifică dacă acestea sunt exacte şi, dacă este cazul, actualizate.

5.7.8. În situaţia în care se constată că au fost transmise date incorecte sau neactualizate TGR are obligaţia de a informa destinatarii respectivelor date asupra neconformităţii acestora, cu menţionarea datelor care au fost modificate.

5.7.9. La comunicarea datelor cu caracter personal TGR atenţionează destinatarii asupra interdicţiei de a prelucra datele pentru alte scopuri decât cele specificate în cererea de comunicare.

5.8. Măsuri tehnice privind prelucrarea datelor cu caracter personal

Toate documentele care conţin date cu caracter personal se înregistrează şi urmează regulile de păstrare, procesare, multiplicare, transport, transmitere, distrugere şi arhivare stabilite prin Legea Arhivelor naţionale şi prin proceduri interne.
Documentele care conţin date cu caracter personal şi care trebuie distruse, se vor trece prin aparatul distrugător de documente (tocător).

Notă:
(1) Acest document se completează cu întreg setul de politici/proceduri de securitate aprobat de conducerea TGR şi aflat în vigoare.

6. DISPOZIŢII FINALE. COMUNICĂRI. CERERI ŞI RECLAMAŢII

6.1. Prezentul document precum şi toate materialele şi informaţiile puse la dispoziţia dumneavoastră sunt proprietatea Travelio Group Romania sau a partenerilor noştri şi sunt protejate prin drepturi de autor, drepturi de marcă şi/sau drepturi de proprietate intelectuală.

6.2. Travelio Group Romania vă stă la dispoziţie pentru orice întrebare sau nelămurire legată de prezentul document. În acest sens, vă încurajăm să ne contactaţi în scris, la adresa de e-mail: office@travelioromania.ro.

6.3. În cazul intervenirii unui litigiu, sub incidenţa legislaţiei române, se va incerca soluţionarea pe cale amiabilă, în termen de 30 de zile calendaristice de la data transmiterii cererii/reclamaţiei către Travelio Group Romania sau, în funcţie de timpii de reacţie ai partenerului/furnizorului etc. căruia ne vom adresa, în cazul în care informaţiile solicitate nu ne sunt disponibile imediat, se va comunica un alt termen de soluţionare.

6.3.1. Cererea/reclamaţia se depune obligatoriu în formă scrisă:

a) prin scrisoare cu confirmare de primire, la adresa de corespondenţă: TRAVELIO GROUP ROMANIA S.R.L., Hunedoara, Bld. Corvin nr. 5 bis, bl. 105, sc. A, ap. 3, parter, 331010, jud. Hunedoara, utilizând şi suportând costurile pentru serviciile Poştei Române sau de curierat rapid (termenul de soluţionare se va calcula începând cu data primirii scrisorii de către Travelio Group Romania);
b) la adresa de e-mail: office@travelioromania.ro; în momentul recepţionării e-mailului dumneavoastră, vă vom transmite un mesaj de tip "Reply", pentru confirmare de luare la cunoştinţă a cererii/reclamaţiei (termenul de soluţionare se va calcula începând cu data recepţionării e-mailului de către Travelio Group Romania).

6.3.2. Rezoluţia cererii/reclamaţiei va fi înaintată către dumneavoastră, pe cale scrisă, pe costul nostru, prin una dintre cele două opţiuni menţionate la art. 6., alin. 6.3.

6.4. Procedura de soluționare alternativă a litigiilor (entitatea SAL):

a) Călătorul are posibilitatea să apeleze și la entitatea de soluționare alternativă a litigiilor (entitatea SAL), care soluționează litigiile în conformitate cu O.G. nr. 38/2015 privind soluţionarea alternativă a litigiilor dintre consumatori și comercianți, precum și la platforma europeană de soluţionare online a litigiilor (platforma SOL) în temeiul Regulamentului (UE) nr. 524/2013 al Parlamentului European;
    i) soluţionarea alternativă a litigiilor (SAL) reprezintă un mecanism alternativ sistemului judiciar, prin care consumatorilor li se oferă posibilitatea de soluţionare a litigiilor pe care le pot avea cu comercianţii, atunci cand se confruntă cu o problemă legată de achiziţionarea unui produs sau serviciu; astfel, reclamaţiile împotriva comercianţilor sunt prezentate voluntar de către consumatori, urmând a fi soluţionate într-un mod independent, imparţial, transparent, rapid şi echitabil;

ii) Direcţia de soluţionare alternativă a litigiilor (Direcţia SAL) din cadrul Autorităţii Naţionale pentru Protecţia Consumatorilor (ANPC) are competenţa să soluţioneze alternativ litigii naţionale şi transfrontaliere izvorâte din contractele de vânzari sau din contractele de prestări servicii încheiate cu un comerciant care desfăşoară activităţi în România, în sectoarele de activitate în care ANPC este competentă.

b) Cererea de aplicare SAL, lista de consilieri SAL, procedura SAL şi legislaţia aplicabilă pot fi consultate aici: https://anpc.ro/categorie/1271/sal.

6.5. Alte date utile în situaţia unor litigii în timpul desfăşurării serviciilor:

- Asociaţia de apărare a drepturilor consumatorilor la nivel global: www.ftc.gov;
- Servicii consulare: www.econsulat.ro.

6.6. Călătorul/reprezentantul călătorului/partenerul de afaceri/angajatul declară în mod expres faptul că îşi asumă interdicţia de a face publicitate negativă societăţii Travelio Group Romania S.R.L. precum şi serviciilor prestate de către acestea, fără ca procedura de înregistrare şi soluţionare a reclamaţiilor prevăzută mai sus să fi fost îndeplinită. Nerespectarea acestei prevederi dă dreptul Travelio Group Romania S.R.L. să solicite Înstanţei despăgubiri corespunzătoare prejudiciului suferit.

6.7. Orice comunicare cu furnizorul/agenţia organizatoare (alta decât Travelio Romania)/prestatorul de servicii/unitatea de cazare etc. se va efectua în mod obligatoriu prin intermediul Agenţiei Travelio Romania precum şi orice cerere/reclamaţie se va depune/transmite în mod obligatoriu Agenţiei Travelio Romania spre soluţionare, cu cel puţin 7 zile calendaristice înainte de data prestării serviciilor turistice contractate.

6.7.1. Pentru toate comunicările, cererile şi reclamaţiile în care Agenţia Travelio Romania nu a fost prioritar şi direct contactată de către călător/reprezentantul călătorului, Agenţia Travelio Romania nu îşi va asuma răspunderea în niciun mod cu privire la soluţionarea acestora.

6.7.2. Pentru orice abatere de la prevederile art. 6.7., alin. 6.7.1., responsabilitatea cu privire la soluţionarea oricărei cereri/reclamaţii revine în mod exclusiv călătorului/reprezentantului călătorului şi furnizorului/agenţiei organizatoare (alta decât Travelio Romania)/prestatorului de servicii/unităţii de cazare etc., ca urmare a înaintării respectiv acceptării cererii/reclamaţiei din partea călătorului/reprezentantului călătorului şi a încălcării acordurilor/raporturilor comerciale existente între părţi.

6.8. În imposibilitatea rezolvării litigiului pe cale amiabilă, acesta se va considera, după caz, ca fiind de competenţa Autorităţii Naţionale pentru Protecţia Consumatorului sau a Instanţelor judecătoreşti, din aceeaşi structură administrativă cu sediul social al Travelio Group Romania S.R.L.

6A. Amendamente

Travelio Group Romania îşi rezervă dreptul de a modifica informaţiile/termenii/condiţiile din prezentul document, iar noua versiune va înlocui versiunea actuală, fără o notificare în prealabil. Acolo unde este cazul, rapoartele contractuale încheiate înainte de data modificării unor termeni şi condiţii nu se vor supune efectelor acestor actualizări, cu excepţia taxelor de rezervare/procesare/altor taxe pentru servicii suplimentare, acestea putându-se modifica în funcţie de politica internă.