REGULAMENT INTERN PRIVIND GESTIONAREA DATELOR

HOTEL TARNAVA 2000 SRL

Valabil de la: 25 mai 2018
Apropat: Bíró-László Zoltán
Clasificarea datelor: NC-01 - Public

RO 535600 Odorheiu Secuiesc,
Piața Városháza nr. 16
+40 266 213 963
www.hoteltarnava.ro
office@kukullo.ro

Cuprins

Introducere

Obiectivul acestui regulament intern privind gestionarea datelor cu caracter personal este de a asigura angajaţilor și colaboratorilor **HOTEL TARNAVA 2000 SRL** (denumită în continuare **HOTEL** sau **compania**) o sinteză ale celor mai importante informații legate de activitatea de gestionare de date efectuate de HOTEL TARNAVA 2000 SRL.

Totodată prezentul document nu se consideră o consultare individuală și substituie auditul protecției datelor. Scopul acestui document este reglementarea internă și asigurarea de asistență și ghidare generală a personalului HOTEL, în vederea asigurării conformării cu cerințele privind protecția datelor.

De-a lungul desfăşurării activităţii HOTEL gestionează diferite date cu caracter personal ale diferitelor grupuri de persoane fizice, cum ar fi:

- persoanele care aplică pentru un loc de muncă,
- angajaţii săi,
- foşti angajaţi,
- delegații furnizorilor cu care HOTEL derulează activități economice, altele decât persoanele cu drept de reprezentare statutară;
- clienţi care participă la anumite promoţii ale societăţii,
- clienții persoane fizice care apelează la serviciile HOTEL prin intermediul vânzărilor retail și/sau web-shop

În ceea ce priveşte colectarea și gestionarea de date ale acestor persoane, HOTEL trebuie să respecte legislația europeană și națională privind protecția datelor cu caracter personal. În acelaşi timp trebuie să țină seama de propriile sale interese de afaceri, condiții operaționale, oportunități tehnice și organizatorice respectiv interesele angajaților și clienților săi.

Obiectivul acestui regulament este de a prezenta pe scurt legislația aplicabilă și măsurile pe care Societatea le ia pentru a respecta legea. Scopul HOTEL este de a asigura întotdeauna că GDPR este respectat într-un mod clar și verificabil.

Acest regulament se aplică tuturor sistemelor, persoanelor și proceselor care constituie sistemul de informații HOTEL, inclusiv conducerea, angajații, furnizorii și alte părți terțe care au acces la sistemul Societății.

1. Regulamentul General privind Protecţia Datelor

Regulamentul General privind Protecţia Datelor nr. 2016/679/UE (***GDPR)*** este cea mai importantă normă legislativă care influențează desfăşurarea activității noastre de gestionare a datelor. Regulamentul comunitar produce efecte în toate statele membre ale Uniunii Europene, prin urmare se aplică în România fără implementare.

1.1 Gestionarea şi procesarea datelor

Având în vedere activitatea HOTEL acesteia i se aplică regulamentul privind protecția datelor. După cum reiese din următoarele concepte ale GDPR, compania și personalul acesteia desfăşoară activităţi de gestionare și prelucrare a datelor.

a) Definiţia *„date cu caracter personal”*:

Datele cu caracter personal reprezintă orice informaţii referitoare la o persoană fizică identificată sau identificabilă (*„persoana vizată”*). O persoană vizată este acea persoană care poate fi identificată, direct sau indirect, în mod particular prin referire la un nume, număr de identificare, date privind locaţia, ID online ori la unul sau mai mulţi factori specifici identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

Prin urmare datele personale reprezintă orice informație pe care HOTEL înregistrează despre o persoană identificată prin digferitele atribute ale persoanei (de exemplu: numărul de telefon, adresa de e-mail, ziua de naștere etc.), deci nu doar datele care permit identificarea propriu zisă a acesteia.

Având în vedere că HOTEL este o societate comercială, în activitatea zilnică are de a face cu date personale, în principal prin intermediul vânzărilor directe (retail și online), respectiv pe cale indirectă, în calitate de delegați, reprezentanți ai partenerilor persoane juridice.

b) definiţia *„gestionarea datelor cu caracter personal”*:

Gestionare de date înseamnă orice operaţiune care se efectuează asupra datelor cu caracter personal, prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terţi prin transmitere, limitarea sau ştergerea;

În consecinţă, de-a lungul desfăşurării activităţii HOTEL gestionează date cu caracter personal.

c) definiţia *„operator”*:

Operator de date se referă la orice persoană fizică sau juridică, care stabileşte scopul şi mijloacele de prelucrare a datelor cu caracter personal.

HOTEL stabilește scopul și mijloacele de gestionare a datelor angajaților și altor persoane și prin urmare se consideră operator de date. Personalul angajat al societății devine operator de date prin exercitarea funcției în cadrul activității desfășurate în cadrul companiei.

d) definiţia *„procesator de date”:*

Procesatorul de date este o persoană fizică sau juridică care procesează date cu caracter personal în numele operatorului de date.

Procesatorii de date de mai jos efectuează activități de gestionare a datelor în numele HOTEL:

Numele celuilalt procesor de date	Adresa	CUI	Descrierea postului de procesor de date
CONTIR CONT S.R.L.	Odorheiu Secuiesc RO-535600, Str. BARTOK BELA 6	RO17180860	Activitati de expertiza contabila
Genetyp Solutions S.R.L.	Cluj Napoca RO-400464 , str. Madach Imre nr. 50	RO14650542	Întreținerea și suportul sistemului (System Hostware);
Service4You Hotel Management Kft.	Budapest H-1022, Fillér u. 84/A	HU01-09-930865	Servicii profesionale de consultanță în exploatarea hotelurilor
Sigma Soft S.R.L.	Odorheiu Secuiesc RO-535600, Str. Izvorului 10	RO526251	Întreținerea IT și supravegherea sistemului (General);

1.2 Principiile gestionării de date

Legislația stabilește principii obligatorii cu privire la gestionarea și prelucrarea datelor, valabil erga omnes.

La gestionarea datelor cu caracter personal se vor avea în vedere și se vor respecta următoarele principii:

1. Datele cu caracter personal:

- gestionarea datelor cu caracter personal se face în conformitate cu prevederile legale, în mod echitabil și transparent (*„legalitate, echitabilitate şi transparenţă”*);
- colectarea se face numai în scopuri bine determinate, explicite şi legitime, şi datele nu vor fi gestionate în moduri incompatibile cu aceste obiective; prelucrarea suplimentară a datelor în scopuri statistice nu se consideră incompatibilitate (*„scopul bine determinat*”);

- trebuie să fie adecvate și relevante pentru gestionarea datelor și trebuie să fie limitate la cât este absolut necesar („*economisire*”);

- să fie corecte și, dacă este necesar actualizate; datele cu caracter personal incorecte trebuie să fie eliminate sau corectate cât mai curând în măsura în care este posibil, ("*exactitate*");

- stocarea trebuie să aibă 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 ori în scopuri statistice, 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”);

- trebuie să fie gestionate 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”).

- respectarea acestor principii trebuie, de asemenea, să fie recunoscută de către operatorul de date („*răspundere*”).

1.3 Gestionarea categoriilor speciale de date cu caracter personal

Conform temeiurilor legale detaliate la articolul 9 din GDPR compnia gestionează uneori categorii speciale de date (de exemplu date privind sănătatea). Gestionarea acestor categorii de date se face pe motive de prevenţie în ceea ce priveşte sănătatea sau sănătatea la locul de muncă (de exemplu gestionarea rezultatelor analizei capacității unui angajat sau acordarea de beneficii persoanelor cu handicap).

Dacă apare necesitatea de a gestiona o categorie specială de date alta decât cele de mai sus, este necesară o examinare preliminară a temeiului legal.

1.4 Drepturile persoanelor vizate

În ceea ce priveşte datele cu caracter personal gestionate de societate, GDPR oferă persoanelor vizate un număr de privilegii care apar ca o obligație pentru companie. Aceste drepturi sunt următoarele:

Dreptul la informare

Persoana vizată are dreptul de a fi informată cu privire la sursa datelor cu caracter personal, scopul, durata stocării, baza legală a gestionării, identitatea procesatorului, felul interesului legitim, transferul de date către țări terțe, destinatarii datelor și categoriile de destinatari în cazul unor interese legitime.

Dreptul la acces

Persoana vizată are dreptul de a primi o informare completă de la operatorul de date cu privire la scopul și modalitatea gestionării datelor sale cu caracter personal și, în cazul în care o astfel de gestionare are loc, are dreptul de a avea acces la datele și inofrmațiile intrinseci ale datelor sale cu caracter personal și la informațiile conexe pe care le administrează.

Dreptul la rectificare

Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

Dreptul la ştergere

Persoana vizată are dreptul să solicite operatorului să-i șteargă datele cu caracter personal fără întârzieri nejustificate, iar operatorul de date este obligat să execute ştergerea (în unele cazuri speciale - articolul 17 din GDPR) dacă scopul sau temeiul legal al gestionării datelor a încetat, gestionarea datelor a avut loc fără niciun temei legal.

Dreptul la restricţionarea gestionării de date

În cazuri specifice prevăzute la articolul 18 din GDPR, persoana vizată poate solicita restricţionarea privind prelucrarea datelor. Restricția înseamnă că operatorul va stoca datele în cauză în continuare, însă le poate gestiona numai cu consimțământul persoanei vizate sau în vederea validării de drepturi ale persoanei vizate sau ale opertorului, legat de persoana vizată.

Obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în conformitate cu prevederile articolului 16, articolul 17 alineatul (1) și articolul 18 din Regulament, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

Dreptul la portabilitatea datelor

Persoana vizată are dreptul de a solicita emiterea datelor sale personale de către Operator într-o formă lizibilă și/sau accesibilă în scopul portării, având dreptul de a transfera aceste informații unui alt operator de date, fără ca prin această portare interesele sau informațiile aparținând unei terțepersoane să fie lezate.

Dreptul la opoziție

Persoana vizată are dreptul de a se opune, din motive legate de situația particulară în care se află, prelucrării a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor dispoziții. Operatorul nu mai prelucrează datele cu caracter personal, cu excepția cazului în care operatorul demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță. Dreptul la opoziție și condițiile de prelucrare vor fi aduse la cunoștința persoanei vizate cel târziu la momentul primei comunicări cu aceasta.

Drepturile legate de crearea de profil şi luarea deciziilor automate

Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.
De asemenea GDPR stabileşte termene pentru obligațiile Companiei care decurg din drepturile persoanei vizate enumerate la 1.4. În cursul executării procedurilor, colaboratorii responsabili ai companiei trebuie să ia în considerare și aceste termene.

Aceste termene sunt prezentate în tabelul de mai jos:

Obiectul cererii persoanei vizate	Termen
Dreptul la informare	la colectarea datelor (dacă sunt furnizate de persoana vizată) sau într-o lună (dacă nu sunt furnizate de persoana vizată)
Dreptul la acces	o lună
Dreptul la rectificare	o lună
Dreptul la ştergere	fără întârzieri nejustificate
Dreptul la restricţionarea gestionării de date	fără întârzieri nejustificate
Dreptul la transferabilitatea datelor	o lună
Dreptul la opunere	La primirea opunerii
Drepturile legate de crearea de profil şi luarea deciziilor automate	nu este stabilit

Societatea trebuie să ia toate măsurile rezonabile pentru a se convinge de identitatea persoanei vizate care dorește să solicite acces sau să-şi exercite drepturile persoanei vizate.

1.5 Temeiuri legale aplicate în activitatea privind gestionarea datelor de către HOTEL

În gestionarea datelor personale raportat la necesitățile impuse de activitatea HOTEL cele mai frecvente temeiuri legale în privinţa gestionării datelor sunt consimțământul, executarea contractului, interesul societății și obligația care decurge din prevederile legale. În toate procesele de gestionare a datelor, temeiul legal pentru gestionarea datelor trebuie identificată în prealabil.

Consimţământul

Pentru activitățile de vânzări online și marketing ale societăţii (newsletter, campanie telefonică, informare prin SMS, etc.), este necesar ***consimțământul*** prealabil al părții vizate. În cazul copiilor sub 16 ani, este necesară permisiunea reprezentantului său legal.

Înainte de primirea consimțământului, trebuie furnizate informații transparente celor vizaţi în legătură cu modul în care informațiile lor personale sunt gestionate, trebuie să fie prezentate drepturile lor în acest sens, în special dreptul de a-și retrage consimțământul dat. Aceste informații trebuie furnizate într-o formă accesibilă, în limbaj simplu și gratuit.

Dacă datele cu caracter personal nu sunt obținute direct de către societate, aceste informații trebuie furnizate persoanei vizate într-un termen cât mai scurt de la obținerea datelor, dar nu mai târziu de o lună.

Consimțământul, inclusiv detaliile datelor persoanei vizate, respectiv locul unde şi data când consimţământul a fost dat trebuie întotdeauna înregistrat și păstrat de către societate în conformitate cu *Regulamentul de stocare și ştergere a datelor.*

Executarea contractului

Datele cu caracter personal furnizate la încheierea contractului sunt necesare pentru executarea contractului de către societate. Acest interes reprezintă o bază juridică suficientă pentru gestionarea datelor cu caracter personal. Interesul rămâne valabil până când interesele legitime legate de executarea contractului pot fi executate – adică până la expirarea termenului de cinci ani după executarea contractului, potrivit codului civil. Totodată este important ca acest consimţământ să se refere exclusiv la datele cu caracter personal necesare pentru executarea contractului, urmând ca aceste date (număr telefon, email, etc) să fie eliminate (șterse) din registrele și evidențele societății.

Îndeplinirea obligaţiei legale ale Companiei

Îndeplinirea obligaţiilor legale ale operatorului de date pot impune gestionarea datelor personale (de exemplu, în calitate de angajator trebuie să gestioneze anumite informații despre angajați, cum ar fi numele, adresa, numărul de identificare fiscală și codul numeric personal etc. pentru a-şi îndeplini obligaţiile legate de depunerea declaraţiilor fiscale şi plata impozitelor, salarii etc.).

Urmărirea drepturilor legitime proprii ale societății sau drepturilor aparținând terțelor persoane

Temeiul legal al gestionării datelor poate fi, de asemenea, necesitatea de a asigura respectarea intereselor legitime ale Companiei sau ale unei terțe părți. În cazul gestionării datelor bazate pe un interes legitim, se va evalua raportul interesului legitim care trebuie aplicat este mai presus de obligativitatea și scopul protecției datelor cu caracter personal. Compania este obligată să prezinte evaluarea relevantă. Un astfel de interes este implicat în decizia angajatorului de supraveghere al angajaților și clienților săi cu o cameră de supraveghere pentru a preveni sau detecta eventualele furturi / fraude. În cazul acesta trebuie să se facă o evaluare adecvată cu privire la drepturile angajaţilor și clienţilor vizaţi, şi trebuie asigurate garanții adecvate pentru protecția vieții private a salariaților, persoanele vizate fiind în mod obligatoriu informaţi cu privire la existența, locația camerelor respectiv modalitatea și locația de stocare a datelor. De asemenea, după evaluarea prevalării intereselor, în cazuri justificate, angajatorul poate accesa corespondența angajatorului din poșta electronică utilizată pentru îndeplinirea sarcinilor de serviciu, în cazul în care există suspiciuni de încălcare a obligațiilor asumate de salariat, respectiv în măsura în care informațiile ale căror recuperare se urmărește aparțin angajatorului sau reprezintă un potențial de produce efecte juridice care vizează angajatorul sub orice aspect. În acest caz, este necesar să se asigure că angajații pot fi prezenți atunci când contul lor de e-mail / utilizarea internetului sau a telefonului este verificat în timpul unui audit.

Protecţie integrată a datelor

Conform reglementărilor GDPR, procesul de gestionare a datelor trebuie să includă principiile de bază și protecția adecvată a drepturilor celor vizaţi. În plus față de crearea unor condiții adecvate de gestionare a datelor, aceste condiții vor fi supuse revizuirilor periodice, în concordanță cu necesitățile impuse reale ale societății, adaptate evoluției tehnologiilor utilizate, schimbărilor intervenite în gestionarea datelor și noilor procese de gestionare a datelor. În funcție de evoluția științei și tehnologiei și de costurile de implementare, precum și de natura, scopul, circumstanțele și obiectivele gestionării datelor, precum și de riscurile cu privire la drepturile și libertățile persoanelor fizice, operatorul de date ia măsuri tehnice și organizatorice adecvate, atât în definirea modului de gestionare a datelor, cât și pe parcursul gestionării - cum ar fi un pseudonimizare - pentru punerea efectivă în aplicare a principiilor protecției datelor, cum ar fi economisirea datelor și includerea garanțiilor necesare pentru a îndeplini cerințele prezentului regulament și pentru a proteja drepturile persoanelor vizate. Operatorul de date adoptă măsuri tehnice și organizatorice adecvate pentru a se asigura că sunt prelucrate numai date cu caracter personal care sunt necesare pentru scopul specific al gestionării de date. Această obligație se referă la cantitatea de date personale colectate, amploarea gestionării, durata stocării și disponibilitatea acestora. Aceste măsuri trebuie să garanteze, în special, că datele cu caracter personal nu sunt puse la dispoziția unui număr nedeterminat de persoane în mod implicit fără intervenția unei persoane fizice.

Compania a luat la cunoştinţă principiul integrat al protecţiei datelor și asigură faptul că acordă atenția cuvenită protecției datelor, realizează evaluările impactului asupra protecţiei datelor în cazul implementării unor modificări ale sitemelor de stocare date (upgrade) și/sau sisteme noi care colectează sau gestionează informații personale.

În plus, Compania va revizui periodic funcționarea sistemelor de gestionare a datelor pentru a se asigura că acestea corespund cu necesitățile actuale pentru care acestea au fost create, respectiv normele legale aplicabile în acel moment sunt respectate.

În vederea aplicării corespunzătoare a prevederilor GDPR privind gestionarea datelor, societatea asigură, că:

- toți membrii personalului implicați în gestionarea datelor cu caracter personal înțeleg responsabilitatea referitoare la monitorizarea bunelor practici de protecție a datelor,
- toţi membrii personalului beneficiază de cursuri privind protecția datelor,
- persoanele vizate au la dispoziţie date de contact ușor accesibile în cazul în care aceştia vor să-şi exercite drepturile cu privire la datele cu caracter personal, și gestionează aceste solicitări în mod eficient.

1.6 Transferul datelor personale

Transferul datelor cu caracter personal în afara Uniunii Europene trebuie verificată cu atenție înainte de transmitere, astfel încât transferul să aibă loc în limitele stabilite de GDPR. Acest lucru depinde parțial de modul în care Comisia Europeană evaluează conformitatea garanțiilor privind datele cu caracter personal în țara de destinație, care pot suferi modificări pe parcursul aplicării.

1.7 Procesatori de date

GDPR prevede că necesitățile proprii de stocare și procesare de date pot fi realizate prin intermediul acelor procesatori de date, care oferă garanții suficiente pentru a introduce măsuri tehnice și organizatorice care să îndeplinească cerințele GDPR, asigurând securitatea datelor și trasabilitatea schimbului de date în sistemele proprii.

În cazul procesatorilor de date din afara Spațiului Economic European, cum ar fi părţi terţe care asigură stocare de date în cloud sau alte tipuri de stocare date, este esențial ca aceste contracte încheiate cu astfel de părţi terţe să includă Termeni și condiții generale pentru gestionarea datelor, în conconrdanță cu regulile specifice trasate de societate pentru gestionarea acestor date.

1.8 Notificarea încălcării drepturilor

Compania este obligată să stabilească în baza principiilor echității și proporționalității, modul și termenul conform cărora va informa persoanele vizate în cazul încălcării cu privire la datele cu caracter personal (incident de protecție a datelor).

În cazul unui incident de protecție a datelor care poate rezulta efecte asupra drepturilor și libertăților persoanelor fizice în termenii definiți de GDPR, autoritatea competentă pentru protecția datelor trebuie informată în termen de 72 de ore.

Procedura de urmărit este cea conformă cu prevederile *Regulilor de gestionare a incidentelor*, stabilind întregul proces de gestionare a incidentelor de securitate a informațiilor.

Încălcarea normelor de securitate a datelor personale atrage sancțiunea prevăzută de GDPR, sancțiunea aplicată de autoritatea competentă pentru protecția datelor constă în amendă de până la 4% din cifra de afaceri totală anuală sau 20 de milioane EUR.

1.9 Limitarea perioadei de stocare a datelor personale

HOTEL va concepe o procedură proprie pentru satbilirea procedurilor de stocare și de ștergere a datelor personale recepționate și utilizate confrom obiectului de activitate. În elaborarea acestor proceduri se vor respecta principiile generale GDPR, îndeosebi principiul legalității, scopului și economisirii.
Regulile privind procesarea în timp a datelor de către HOTEL sunt reglementate de *Regulamentul de stocare și ştergere a datelor.*

1.10 Obligaţii privind păstrarea evidenţei

GDPR prevede obligativitatea ținerii evidenţelor legate de activitățile de gestionare a datelor cu caracter personal în cazurile în care gestionarea datelor nu este ocazională. Modalitatea de evidențiere a activităților HOTEL în care sunt implicate date personale este reglementată prin Evidenţa de gestionare a datelor.

Evidenţa de gestionare a datelor reflectă modalitatea de respectare de către HOTEL a principiilor statuate prin GDPR cu referire la:

- temeiul legal privind gestionara datelor cu caracter personal este întotdeauna clară și lipsită de ambiguitate,
- scopul gestionării datelor este bine definit, sfera datelor gestionate este necesară pentru atingerea scopului,
- persoana vizată a fost informată în mod corespunzător cu privire la gestionarea datelor,
- durata gestionării datelor şi ştergerea sunt reglementate,
- stocarea datelor are loc cu respectarea măsurilor de securitate corespunzătoare,
- transferul de date are loc cu asigurare de garanţii corespunzătoare,
- persoana responsabilă pentru gestionarea datelor a fost desemnată.

2. Responsabilitatea privind gestionarea datelor

Siguranța datelor personale constituie o prioritate deosebită în activitatea HOTEL. Pentru a asigura cadrul instituțional de urmărire și control a modalității de respectare a regulamentelor și măsurilor aplicate precum și a eficienței acestora, în cadrul societății sunt auditate aspectele privind: identificate sursele posibile de proveniență a datelor personale, căile de recepție a acestor date, trierea datelor, stocarea și managementul de date conform scopului declarat pentru care s-a obținut consimțământul titlarului, durata de prelucrare și stocare, eliminarea datelor ale căror termen sau utilitate a expirat. În scopul asigurării unei gestiuni echitabile și legale, HOTEL desemnează persoanele responsabile din cadrul societății pentru supravegherea procedurilor de gestionare a datelor precum şi sarcinile pe care această responsabilitate de supraveghere implică.

Acest document trebuie citit și aplicat împreună cu alte documente referitoare la activitățile de gestionare a datelor din cadrul societății, cum ar fi:

- *regulamentul intern privind gestionarea datelor;*
- *procedura de notificare a încălcărilor privind datele cu caracter personal (incidente de protecţia datelor); şi*
- *procedura de gestionare a cererii persoanei vizate.*

Definirea clară a rolurilor și responsabilităților, reglementarea adecvată a sarcinilor relevante urmărește prevenirea apariției incidentelor privind protecţia datelor personale și permite luarea unor măsuri eficiente și adecvate în cazul apariției unor asemenea incidente.

2.1 Reguli referitoare la protecţia datelor

În vederea respectării regulilor și normelor legale incidente în materie, HOTEL va stoca și procesa datele necesare realizării obiectivelor sale în mod legal și echitabil, urmând ca angajații implicați în aceste proceduri să fie implicați în următoarele calități arondate:

- Operator de date
- Manager pentru securitatea informațiilor
- Responsabil pentru conformitate

Responsabilitățile specifice ale fiecărui rol sunt descrise în continuarea în acest document.

Toţi angajații și partenerii Companiei care desfășoară activități de gestionare a datelor sunt obligați să îndeplinească sarcinile și obligațiile de mai jos pentru a asigura aplicarea în mod corespunzător a principiilor generale GDPR, precum principiul gestionării legitime, corecte și transparente a datelor, principiul scopului bine stabilit, principiul economisirii și exactităţii datelor și principiul integrității și al confidențialității.

Prezentul Regulament stabilește responsabilitățile fiecărei calități în cadrul procedurilor GDPR din organizația HOTEL, fără ca aceste calități să producă efecte asupra funcției, sracinilor sau competențelor generale ale angajatului, care nu sunt legate de GDPR și nu poate fi considerată o fișă completă a postului.

2.1.1 Operator de date

Conform prevederilor GDPR, operatorul de date este *o persoană fizică sau juridică, o autoritate publică, o agenție sau orice alt organism care singur sau împreună cu altele stabileşte scopurile și mijloacele de prelucrare a datelor cu caracter personal.*
Operatorul de date are în principiu următoarele responsabilităţi:

- Asigură conformitatea cu principiile stabilite la articolul 5 din GDPR a modalității de gestionare a datelor cu caracter personal, asigurând posibilitatea verificării și demonstrării modalității de realizare a acestora. Prin urmare, asigură că informațiile personale:

  (i) sunt gestionate în mod legal, corect și transparent,
  (ii) sunt colectate în funcţie de obiectivele definite, concrete şi legitime,
  (iii) sunt limitate la cele adecvate, relevante şi necesare,
  (iv) sunt exacte şi, dacă este necesar, actualizate,
  (v) sunt stocate în aşa fel încât să permită identificarea persoanelor vizate doar atât timp cât este necesar,
  (vi) sunt gestionate în siguranţă adecvată.

- Asigură obţinerea consimțământului persoanei vizate în ceea ce privește gestionarea datelor cu caracter personal, inclusiv consimțământul părinţilor în cazul copiilor.

- Pune la dispoziţia persoanei vizate toate informațiile prevăzute de GDPR într-o formă concisă, transparentă, ușor de înțeles și ușor accesibilă, într-un limbaj simplu și clar.

- Permite exercitarea drepturilor conferite de GDPR de către persoanele vizate și le informează cu privire la prelucrarea cererii sale. În acest sens, persoanele vizate au dreptul de a accesa datele colectate despre ele și au dreptul de a verifica legalitatea gestionării datelor. De asemenea, pot primi informaţii despre durata gestionării datelor, consecințele gestionării datelor (cum ar fi identificarea profilului), logica gestionării datelor.

- Asigură că va colabora doar cu procesatori de date care oferă garanția corespunzătoare că se vor lua măsurile tehnice și organizatorice adecvate pentru a respecta GDPR și proteja datele personale
- Ţine evidența activităților de gestionare a datelor cu caracter personal, ceea ce este responsabilitatea operatorului de date.
- La cerere cooperează cu autoritatea de supraveghere în vederea îndeplinirii sarcinilor sale.

- Asigură că orice persoană care acționează în numele operatorului de date care are acces la datele cu caracter personal, gestionează informaţiile numai în conformitate cu instrucțiunile operatorului de date.

- Notifică autoritatea de supraveghere fără întârzieri nejustificate cu privire la orice încălcare a drepturilor privind datele cu caracter personal, cu excepția cazului în care este puțin probabil ca încălcarea datelor cu caracter personal să reprezinte un risc pentru drepturile și libertățile persoanelor fizice, în conformitate cu procedurile organizaționale.

- Documentează orice încălcare a drepturilor privind datele cu caracter personal, inclusiv fapte legate de încălcarea datelor cu caracter personal, efectele acestora și măsurile corective luate.

- Dacă este cazul informează persoana vizată fără întârzieri nejustificate cu privire la încălcarea drepturilor privind datele cu caracter personal.

- Efectuează o evaluare a impactului privind protecția datelor, după caz, în conformitate cu procedurile.

- În îndeplinirea sarcinilor sale este susţinut de responsabilul pentru conformitate care îi asigură resurse necesare îndeplinirii sarcinilor şi accesării şi gestionării datelor cu caracter personal respectiv îl ajută din punct de vedere profesional.

- Datele cu caracter personal pot fi transferate unei țări terțe sau unei organizații internaționale, în cazul în care operatorul de date sau un procesator de date a

furnizat garanții adecvate și cu condiția ca drepturile persoanelor vizate să fie respectate și să fie disponibile căi de atac eficiente.

2.1.2 Manager pentru securitatea informațiilor

Sarcina principală a Managerului pentru Securitatea Informațiilor este elaborarea și menținerea securității informațiilor. Responsabilitățile Managerului pentru Securitatea Informațiilor sunt următoarele:

- Elaborează și prezintă conducerii măsurile ce trebuie luate pentru asigurarea securității informațiilor;
- Conduce implementarea deciziilor luate de conducere pentru a asigura securitatea informațiilor;
- Supraveghează funcționarea sistemului de securitate a informațiilor;
- Identifică, cuantifică și monitorizează tipurile, amploarea și impactul incidentelor și erorilor de funcţionare și ia măsurile necesare pentru prevenirea și soluționarea acestora;
- Întocmeşte rapoarte în mod regulat și, dacă este necesar după caz, conducerii în legătură cu gestionarea tuturor aspectelor legate de siguranță;
- Colaborează cu Responsabilul pentru conformitate și execută instrucțiunile acestuia;
- Informează persoana vizată despre regulamentul de securitate a informațiilor;
- Execută prevederile regulamentului privind securitatea informațiilor;
- Se ocupă de managementul riscurilor legate de accesul la servicii sau sisteme;
- Asigură aplicarea și documentarea controalelor de securitate;
- Stabilește planurile de dezvoltare și obiectivele pentru exercițiul financiar;
- Monitorizează realizarea planurilor de dezvoltare.

2.1.3. Responsabil cu protecția datelor

Responsabilitățile Responsabilului pentru protecția datelor sunt următoarele:

- Furnizează informații și consultanță profesională operatorului de date sau procesatorului de date respectiv angajaţilor responsabili pentru gestionarea datelor

cu privire la obligațiile care le revin în temeiul legislației aplicabile privind protecția datelor;

- supraveghează respectarea legislației privind protecția datelor și a regulamentului intern privind protecția datelor cu caracter personal de către operatorul de date sau procesorul de date;
- elaborează și menține regulamente interne și externe privind protecția datelor, reglementări privind securitatea informațiilor, obiective și planuri;
- atribuie responsabilități, contribuie la creşterea gradului de conştientizare a personalului în operațiunile de gestionare a datelor, instruieşte personalul și efectuează audituri conexe;
- la cerere oferă consultanță profesională privind evaluarea impactului privind protecția datelor și monitorizează evaluarea impactului;
- cooperează cu autoritatea de supraveghere competentă pentru protecția datelor;
- este persoana care ţine legătura cu autoritatea de supraveghere în subiecte legate de gestionarea datelor şi dacă este cazul o consultă legat de orice alt subiect.
- asigură că cerințele legale și de securitate a informațiilor sunt stabilite și îndeplinite pentru a minimiza riscul și a utiliza controale eficiente în cadrul companiei în ceea ce priveşte clienții;
- stabileşte resursele pentru planificarea, implementarea, supravegherea, revizuirea și dezvoltarea în ceea ce priveşte respectarea prevederilor legale, securitatea și gestionarea informațiilor și ia măsuri pentru asigurarea acestora (de exemplu, angajarea personalului adecvat și gestionarea fluctuației personalului);
- supraveghează gestionarea riscurilor care afectează organizația și serviciile acesteia;
- periodic efectuează revizuirea securității informațiilor din punct de vedere al aptitudinii, conformităţii şi eficienţei;
- examinează incidentele majore privind securitatea informațiilor;
- asigură ca accesul organizațiilor externe la sistemele informatice să se bazeze pe un acord oficial care stabilește toate cerințele legale și de siguranță necesare.

Societatea va examina în mod permanent oportunitatea și actualitatea desemnării unui Responsabil cu protecția datelor urmând ca în baza acestor concluzii să desemneze / sau nu resposnabilul.

2.1.4 Angajaţi

Responsabilitățile principale ale angajatului sunt următoarele:

- Cunoaşte şi respectă toate regulamentele organizaţiei legate de protecţia datelor, implicate de rolul său.
- Raportează orice incidente reale sau potențiale legate de protecţia datelor.
- Dacă este necesar contribuie la evaluarea impactului privind protecția datelor.