

RGPD

1. Audit date personale si sensibile

1.1 Date personale colectate de **SC DE MAR SPECIAL SRL**

- Nume si prenume (pentru minori sau persoane care nu se pot reprezenta singura si numele si prenumele reprezentantului legal)
- Varsta (nu data nasterii)
- Numar de telefon
- Adresa de e-mail
- Adresa de corespondenta

1.2 Metode de colectare de date personale

- Inregistrare clienti (prin aplicatiile electronice de gestiune)
- Inregistrare programare
- Fisele de acord informat al clientului
- Facturi emise catre clienti
- Dosarele de angajati

1.3 Metode de colectare de date cu caracter sensibil

- Inregistrare clienti prin aplicatiile electronice de gestiune
- Date primite de la terti
- Fisele de acord informat al clientului
- Facturi emise catre clienti
- Inregistrare audio-video prin robot telefonic si prin inregistrare audio

2. Informare persoane vizate (anexa informare)

2.1 Tipuri de informare

2.1.1 In format fizic in receptie

- 2.1.2 On-line – in site (buton pe site cu redirectionare catre anexa de informare) si in e-mailurile trimise clientilor (mesaj scris scurt la finalul oricarui e-mail trimis catre persoanele vizate).

2.2 Responsabil cu protectia datelor

Responsabilul cu protectia datelor este Vieru Dana. In lipsa ei responsabili sunt in ordine in functie de disponibilitate: Hutanu Vanessa, Vasluianu Casian si Vasluianu Marinel.

- 2.3 Date colectate – incluse in informare
- 2.4 Scopul colectarii – incluse in informare
- 2.5 Durata colectarii – incluse in informare
- 2.6 Terti catre care sunt divulgate informatii – incluse in informare
- 2.7 Drepturi persoane vizate – incluse in informare
- 2.8 Proceduri de pastrare, evidente, arhivare – incluse in informare
- 2.9 Temeiuri legale – incluse in informare
- 2.10 Securitatea datelor – incluse in informare
- 2.11 Inregistrarea audio-video – incluse in informare
- 2.12 Colectarea in scopuri de marketing – incluse in informare
- 2.13 Informatii cu caracter general despre informare

3. Proceduri personal

3.1 Colectare date

Datele pot fi colectate de personalul angajat sau in relatii de colaborare cu SC DE MAR SPECIAL SRL sau pot fi primite de la terti.

Colectarea de date, trebuie sa se rezume doar la acele date esentiale inregistrarii clientului pentru prestare a serviciului solicitat.

Personalul nu are voie sa colecteze date cu caracter sensibil, altele decat imagini video si inregistrare audio.

Colectarea de date va include date cu caracter personal limitate (nume, prenume si varsta).

3.2 Stocare date

3.2.1 Datele stocate in format virtual

Datele stocate in format virtual sunt urmatoarele:

- Inregistrarile audio realizate de robotul telefonic
- Facturi emise catre clienti

Datele sunt stocate pe serverul intern – securizat prin antivirus si sisteme de back-up interne.

3.2.2 Date stocate in format fizic

Datele stocate in format fizic sunt urmatoarele:

- Consimtamintele informate ale clientilor
- Facturi emise pentru clienti
- Dosarele angajatilor
- Dosarele clientilor cu solicitari complexe si care necesita informare speciala

3.3 Gestionare date stocate

3.3.1 Date stocate in format virtual

Datele stocate in mediu virtual pot fi gestionate prin intermediul aplicatiilor electronice de gestiune.

Persoanele care introduc sau acceseaza date deja stocate in format virtual prin orice aplicatie sau dispozitiv, au obligatia sa se delogheze din aplicatie dupa ce au terminat introducerea sau accesarea.

Persoanele care introduc sau acceseaza date deja stocate in format virtual prin orice aplicatie sau dispozitiv, trebuie sa incerce, in limite rezonabile sa nu permita ca datele sa fie vizualizate de persoane care nu au acces la ele.

3.3.2 Date stocate in format fizic

Accesul la datele fizice este limitat la urmatoarele persoane: Vieru Dana, Hutanu Vanessa, Vasluianu Casian si Vasluianu Marinela. Acestea vor accesa

dosarele cu datele fizice pentru persoanele care solicita informatii din ele. Accesul va fi jurnalizat intr-un tabel la inceputul fiecarui dosar in care se vor mentiona urmatoarele:

- Numele persoanei care a accesat datele
- Numele persoanei care a solicitat datele
- Ziua accesarii
- Scopul accesarii datelor
- Durata accesarii

Datele in format fizic vor fi colectate de catre personalul din receptie si depozitate provizoriu pe timpul zilei in camera de stocare din spatele receptiei. La sfarsitul zilei vor fi depuse in dosarele speciale din "Birou".

Orice document in format fizic, emis pentru uzul clientilor, care contine date cu caracter personal sau sensibil si care este deja stocat in format virtual si care nu a fost inmanat clientului sau persoanei imputernicite va fi distrus la sfarsitul fiecarei zile.

3.4 Gestionare spatiu de lucru in vederea asigurarii datelor personale

Toate persoanele care prelucreaza date cu caracter personal sau sensibil au obligatia de a isi gestiona spatiul de lucru astfel incat sa previna scurgerile de informatii. Acestea trebuie:

- Sa se delogheze din orice aplicatie sau program in momentul in care parasesc spatiul de lucru (pentru situatii in care absenta acestuia este mai mare de 15 minute)
- Sa opereze dispozitivele si aplicatiile astfel incat persoanele neautorizate sa nu intre in contact cu datele altor persoane inregistrate
- Sa nu lase la vedere documente care pot sa contina date cu caracter personal sau sensibil
- Sa nu permita accesul persoanelor neautorizate in aplicatiile sau pe dispozitivele cu care se gestioneaza datele cu caracter personal sau sensibil
- Sa nu ofere verbal sau in scris persoanelor neautorizate informatii despre datele cu caracter personal sau sensibil
- Sa utilizeze pentru comunicarea cu clienti doar adrese de e-mail securizate

3.5 Transmitere date

Comunicarea datelor cu caracter personal sau sensibil se va realiza doar dupa ce au fost stabilite identitatea si dreptul persoanei care solicita informatiile.

Toate comunicările cu clienti sau cu terti se vor realiza prin canale de comunicare securizate.

In cazul in care acest lucru nu este posibil se va aduce la cunostinta persoanei sau institutiei in cauza imposibilitatea transmiterii documentelor.

In cazul acceptului expres al clientului sau institutiei in cauza comunicarea se va realiza prin mijloace de comunicare nesecurizate.

4. Proceduri incident - Interventie conform schemei A.1

- a. Constatare
- b. Limitarea efectelor
- c. Remediere